An Endeavour in the Domain of Cybercrime

Exploring the Structural and Cultural Features of the Darknet Market AlphaBay

Åsne Hugdal Kalberg

Autumn 2017

Master's thesis in Criminology

Department of Criminology and Sociology of Law

Faculty of Law

University of Oslo
An Endeavour in the Domain of Cybercrime

Exploring the Structural and Cultural Features of the Darknet Market AlphaBay
An Endeavour in the Domain of Cybercrime: Exploring the Structural and Cultural Features of the Darknet Market AlphaBay

Åsne Hugdal Kalberg

http://www.duo.uio.no/

Trykk: Grafisk Senter, Oslo
Summary

Title: An Endeavour in the Domain of Cybercrime: Exploring the Structural and Cultural Features of the Darknet Market AlphaBay

Author: Åsne Hugdal Kalberg

Supervisor: Sveinung Sandberg

Department of Criminology and Sociology of Law

Faculty of Law

University of Oslo

Autumn 2017

This thesis explores the structural and cultural features of the Darknet market AlphaBay. The main focus is on the cybercrime sections of the market, specifically those dealing in cybercrime tools and services. The Internet, and particularly the Darknet, provides its users with anonymity and therefore has become a new arena for criminal and deviant behaviour. Several studies have been conducted on the online trade of drugs, sexually explicit materials, and other illicit materials and goods, but few have been dedicated to the distribution of cybercrime tools and services. The objectives of this thesis are therefore: to investigate the formal and informal mechanisms that are implemented to regulate the marketplace; to evaluate the possible influence of hacker culture on the market culture of cybercrime markets; and to examine how general market culture is displayed on the marketplace and identify a specific market culture for cybercrime markets.

To answer these objectives a qualitative approach was deemed best, and subsequently a combination of netnography and grounded theory was applied in order to ensure due diligence. The data collected consists of 1175 screenshots taken from both the marketplace and the connected forum. In addition, a research journal was also kept to complement the screenshots collected. It functioned as a means for the researcher to remember the processes such as becoming a member, as well as a way of writing down thoughts and impressions that emerged throughout the fieldwork; much like fieldnotes in traditional ethnography.
The data was analysed within a framework made out of economic sociological contributions, as well as criminological and sociological literature on hacker culture. The backbone of the thesis is largely Aspers’ (2011) distinction between general market culture and specific market culture, which is present in both analysis chapters and further deliberated in the final chapter. In addition, previous criminological, sociological and economic research on online illegal markets form a foundation for comparison, and are discussed throughout the thesis.

The structural features of AlphaBay and the formal and informal mechanisms of regulation are the subject of analysis in chapter five. Here, the coordination problems of illegal markets identified by Beckert and Wehinger (2012) are used as an analytical tool in order to understand how the structural features are designed to tackle these problems of coordination, and to investigate the formal and informal mechanisms implemented. AlphaBay, like many other online legal and illegal markets, had formal mechanisms such as market rules, payment method, staff, trust levels, and a feedback system. These mechanisms, combined with the mechanism of punishment for transgression, are implemented by the administration as a way of regulating the market by ensuring order, trust, efficiency, and transparency. These elements are imitations of legal markets, where the state is the regulating force, legislative measures are implemented to regulate the market actors, and legal recourse is available if someone should be cheated. According to Beckert and Wehinger, illegal markets are structurally inefficient because of their intransparency, but this thesis argues that online illegal markets are more transparent than their physical equivalents, and therefore structurally efficient. In addition, issues of trust are central in illegal online markets, because of their anonymous and secretive nature. These formal and informal mechanisms also indicated trustworthiness of other market actors and thus provided potential buyers with means to make an informed decision on whom to initiate trade with.

Further, the thesis analyses the influence of hacker culture on the market, which is done mainly by analysing the forum threads but also the written comments of the feedback. It is also in this chapter that the specific market culture of cybercrime markets is revealed. Here, elements of technological development, knowledge, and skill are pivotal in order to understand the values of market actors. Members would constantly scrutinise other members’ knowledge and skill of cybercrime tools and services, and their willingness to learn. These are unique to the market culture of cybercrime markets. In addition, the inherently masculine environment is considered to be part of a broader specific market culture that spans other online illegal markets as well as cybercrime markets. The most extreme perpetuation this occurred through ‘flaming’, where members would use misogynistic insults to shame others.
The structural features and mechanisms of enforcement explored on AlphaBay bear resonance to general market culture and have proven to be highly efficient and sophisticated. This thesis therefore expects future online illegal markets to adapt similar, perhaps even improved, structures. Furthermore, the specific market culture of cybercrime markets identified in this thesis proves the fruitfulness of analysing the market culture of online illegal markets; by examining their cultural norms, values, and beliefs, we can understand their behaviour and hopefully also disrupt it.
Acknowledgements

First, I want to express my sincere gratitude to my academic supervisor, Sveinung Sandberg, for your excellent guidance, support, and encouragement throughout this project. I am so grateful for your commitment as a supervisor and for the valuable insights you have provided.

A thank you is also highly in order to my friends and co-students at Domus Nova for all the smiles, tears, and hours of discussions that have made the past two years inspiring. A special thanks to Hans, Magnus, and Julie for your feedback and deliberations in our group session.

Eternal gratitude to my family: my parents, Berit and Thor Inge, for your constant support and unwavering belief in me, I would not have made it this far without you. To Tor Olav and Marius, for always being an inspiration in my life! And to Bjørnar, for the countless phone calls, words of encouragement, reading and re-reading of my work, and for believing in me more than I believe in myself. Your investment in my academic career means more to me than you could ever know. Thank you.

To my uncle Olav, for dedicating your time to proof-read my thesis and doing it with sincere commitment; I am forever grateful.

Thanks also to my tech-savvy cousin, Bjørn, for help and advice when my technical knowledge failed me. And to my cousin and roomie, Ingrid: THANK YOU for bearing with me and my rollercoaster of emotions; I know it hasn’t always been easy.

I would also like to extend my gratitude to my former lecturer of Cybercrime & Society at Kingston University London, Dr Christopher Hamerton, for encouraging me to pursue the subject of cybercrime when my time at KU was at an end. You taught me a great deal and your encouragement inspired me to choose this topic for my master’s thesis.

Last, but definitely not least, a heartfelt thank you to my better half, Vincent, for continuously supporting, encouraging, and inspiring me even though I have spent more time at Domus Nova than at home. You have kept me sane; I would not have made it without you. Thank you for all the questions, thoughts, and discussions; for jump-starting my brain when I was convinced it had stopped working.

August 2017, Oslo

Åsne Hugdal Kalberg
# Table of Contents

1. **Introduction** ........................................................................................................... 1
   1.1 Research Aim and Objectives ............................................................................... 2
   1.2 What is Cybercrime? ............................................................................................. 3
      1.2.1 Typologies ....................................................................................................... 5
   1.3 The Darknet .......................................................................................................... 6
      1.3.1 Tor ................................................................................................................... 7
   1.4 AlphaBay ............................................................................................................... 7
   1.5 Gaps in the Literature .......................................................................................... 8
   1.6 Outline of the Thesis ............................................................................................. 9

2. **Literature Review** .................................................................................................... 11
   2.1 Economic Sociology .............................................................................................. 12
   2.2 Coordination Problems ......................................................................................... 14
      2.2.1 Value ............................................................................................................... 14
      2.2.2 Competition .................................................................................................... 15
      2.2.3 Cooperation .................................................................................................... 16
   2.3 Hacker Culture ....................................................................................................... 17
      2.3.1 Technology ..................................................................................................... 18
      2.3.2 Secrecy .......................................................................................................... 19
      2.3.3 Mastery ......................................................................................................... 20
      2.3.4 Masculinity .................................................................................................... 21
   2.4 Previous Research ................................................................................................. 22
   2.5 Concluding Remarks ............................................................................................. 24

3. **Methodology** ........................................................................................................... 27
   3.1 Research Design and Data Collection .................................................................... 28
      3.1.1 Locating the Field ......................................................................................... 29
3.1.2 Accessing AlphaBay ........................................................................... 29
3.2 The Data ................................................................................................. 31
3.2.1 Primary Data .................................................................................... 32
3.3 Analysis ................................................................................................. 34
3.4 Ethical Considerations ......................................................................... 35
3.4.1 Public versus Private Space .............................................................. 36
3.4.2 Protection of Participants ................................................................. 37
3.4.4 Limitations ....................................................................................... 37
4. Structural Features and Mechanisms of Enforcement ............................. 39
4.1 Becoming a Member ............................................................................. 40
4.2 The Forum and the AlphaBay Staff ..................................................... 42
4.3 Payment method .................................................................................. 43
4.4 Market Rules ....................................................................................... 45
4.5 Levels of Trust .................................................................................... 50
4.6 Feedback .............................................................................................. 53
4.6.1 Feedback Content ........................................................................... 56
4.7 Concluding remarks ........................................................................... 59
5. The Influence of Hacker Culture ............................................................. 61
5.1 Development and Technical Finesse ................................................... 62
5.2 Knowledge and Information ............................................................... 65
5.3 Skill .................................................................................................... 67
5.4 Outsiders ............................................................................................. 68
5.5 Reputation ........................................................................................... 71
5.6 Flaming ............................................................................................... 75
5.7 Masculinity ......................................................................................... 77
5.8 Concluding Remarks .......................................................................... 79
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussion and Conclusion</td>
<td>81</td>
</tr>
<tr>
<td>6.1 General Market Culture</td>
<td>81</td>
</tr>
<tr>
<td>6.2 Specific Market Culture</td>
<td>82</td>
</tr>
<tr>
<td>6.3 Widening the perspective</td>
<td>85</td>
</tr>
<tr>
<td>6.4 Conclusion</td>
<td>87</td>
</tr>
<tr>
<td>Bibliography</td>
<td>91</td>
</tr>
<tr>
<td>Appendix</td>
<td>99</td>
</tr>
<tr>
<td>1. Screenshots</td>
<td>99</td>
</tr>
</tbody>
</table>
1. Introduction

‘Criminal forums or marketplaces within the deep web or Darknet remain a crucial environment for cybercriminals to communicate and are a key component for CaaS [Crime-as-a-Service].’

(SOCTA, 2017: 29)

Cybercrime is a widespread phenomenon of which the contemporary network society (Castells, 2010) is highly fearful. The issues surrounding crimes committed in cyberspace are complex and, in many instances, perplexing. People struggle with wrapping their heads around what constitutes cybercrime and how they can best protect themselves from it, perhaps because many don’t know how the technology they have become so dependent upon works (Holt & Bossler, 2016; Jordan, 2008; Yar, 2013). Technology in general is something that has to be learned, and this is arguably where some of the issues and fears originate. Cybercriminals, specifically when understood to be synonymous with hackers (Décary-Hétu & Dupont, 2013; Yar, 2013: 24), are considered to be technological ‘whiz kids’ with unfathomable know-how of technology (Taylor, 1999; Thomas, 2002; Wall, 2001a; Yar, 2013). Because so many end-users of technology are not tech savvy, the tricks and tools used by cybercriminals are frightening, and in turn, there has developed a kind of moral panic, or ‘culture of fear’, regarding cybercrime (Broadhurst et al., 2014; Furnell, 2010; Sandywell, 2010; Thomas, 2002; Wall, 2007a). However, this fear is not entirely irrational as the threat of cybercrime has been rapidly growing, particularly since the implementation of the World-Wide-Web (Furnell, 2003; Furnell, 2010). In addition, authorities and research organs around the world consider cybercrime as an imminent threat towards both businesses and individuals; a threat that will only increase with time (see NSM, 2016; SOCTA 2017).

Cybercrime has evolved from being a transgression often committed by a particularly skilled individual, to now being something that can be ordered by almost anyone online, either to buy a cybercrime tool or to hire someone to do it for you (also known as Crime-as-a-Service [CaaS])(Ablon & Libicki, 2015; Allodi et al., 2015; Holt et al., 2011). Similarly, the tools used in cybercrime have gone from being used solely by those who build them and their delinquent
peers, to being distributed on markets online\textsuperscript{1}. This development can be viewed as one of the reasons why cybercrime is becoming more and more of a threat, and therefore this distribution of malware and other cybercrime services is important to study. In fact, the European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 report lists cybercrime as being a ‘high threat’ warranting specific priority, and the ‘online trade in illicit goods and services’ as a cross-cutting priority that affects other areas of crime (2017: 57). The quote at the top indicates that marketplaces on the Darknet are central for cybercriminals to communicate and spread their services, which is why studying the structure and culture of such a market is not only necessary, but also academically bountiful. This thesis, therefore, utilises the Darknet market AlphaBay as a source for collecting primary data and develop a deeper understanding for the structural and cultural features of online illegal markets.

1.1 \textbf{Research Aim and Objectives}

The main aim of the thesis is to explore the structural and cultural features of Darknet cybercrime markets, using AlphaBay as a case study. Subsequently, the objectives are:

1. To investigate the formal and informal mechanisms implemented to regulate the marketplace.
2. To evaluate the possible influence of hacker culture on the market culture of cybercrime markets.
3. To examine how general market culture is displayed on the market and identify a specific market culture for cybercrime markets.

The first objective will be tackled in chapter four, the second objective in chapter five and the third objective is discussed throughout both chapters four and five, as well as more thoroughly in chapter six. Considering the nature of the aim and objectives, I will do an empirical study using qualitative research methods; specifically netnography. I have accessed the Darknet via the open-source browser Tor\textsuperscript{2} and collected screenshots of both the marketplace and the AlphaBay Market Forum as primary data. It is important to note that even though AlphaBay is a marketplace that distributes an array of illegal products, the main focus of this thesis has been on the sections

\textsuperscript{1} For details on the development of malware, see Ollmann (2008)

\textsuperscript{2} See section 1.3
dealing in ‘true cybercrime’ (see section 1.2) tools and services. Further details and justification of my methodological approach will be thoroughly discussed in chapter three.

In addition, this thesis draws on contributions in economic sociology to form a theoretical framework in which the primary data will be analysed. The backbone of the study is Aspers’ (2011) distinction between general market culture and specific market culture. In addition, the notion of ‘coordination problems’ faced by market actors as identified by Beckert and Wehinger (2012) is applied in order to identify and understand the structural features of the market. Furthermore, literature on hacker culture, coupled with previous research in the field, is used to determine the specific market culture of cybercrime markets. The previous research done in relation to cybercrime markets and other Darknet markets is also applied in order to conceptualise some of the findings from the analysis and to justify the elements of specific and general market culture recognised on AlphaBay.

Before we dive into the realm of the so-called computer underground and its structural and cultural features, it is essential to clarify some of the concepts presented both in the introduction and throughout the paper. This chapter, thus, sets out to discuss the concept of ‘cybercrime’: the challenges defining it, what it is, and how the term is understood and used in this thesis. Further, the chapter will provide a justification for why this paper utilizes the terms ‘Darknet’ and ‘Clearnet’ as well as an explanation as to what constitutes the Darknet and the tool used to access it (i.e., Tor). In addition, the reader will be briefly introduced to the subject of study, the Darknet market AlphaBay, before an outline of the remainder of the thesis is presented.

1.2 What is Cybercrime?

In the broadest, and sometimes misleading, sense, the term ‘cybercrime’ refers to all kinds of computer-related offences (Holt & Bossler, 2016; Jewkes & Yar, 2010; Wall, 2007a; Wall 2007b; Yar, 2013). It is a contested term and some authors use other terms or concepts in order to comprehend these phenomena of transgressions, for example: computer crime (Holt & Bossler, 2016; Jaishankar, 2007), netcrime (Mann & Sutton, 1998), hypercrime (McGuire, 2007), and e-criminality (Sandywell, 2010). Despite this, ‘cybercrime’ precedes and has not only become entrenched into the popular imagination, but also prevails in academic circles, law enforcement, and policy-making bodies (Furnell, 2003; Holt & Bossler, 2016; SOCTA, 2017; Wall, 2007a; Yar, 2013). Although the terminology has been contested, there seems to be a consensus towards the
fact that there is a need to make a distinction between computer-assisted offenses and computer-focused offenses (Furnell, 2003; Holt & Bossler, 2016; Jewkes & Yar, 2010; Wall 2007a; Wall 2007b; Yar, 2013). Nonetheless, to demonstrate the complexities of the cybercrime phenomenon, there are even here inconsistencies in the terminology amongst scholars. Wall (2007a, 2007b), for example, distinguishes between three categories; computer-assisted crime, computer integrity crime, and computer content crime. Others apply the terms ‘computer-oriented offences’ (Jewkes, 2011; Jewkes & Yar, 2010) and ‘computer-dependent crimes’ (SOCTA, 2017). Unfortunately, it is not within the scope of this paper to go into a detailed discussion about the terminology, but the examples above nevertheless highlight the lack of unanimity. For clarity, I use the terms computer-assisted and computer-dependent to distinguish between the two, of which the latter is the focus of this thesis.

As the terms above indicate, the main distinction between the categories is that some of the offences are what Grabosky (2001) called ‘old wine in new bottles’ (cited in Jewkes & Yar, 2010: 3; Jewkes, 2011; McGuire, 2007). At its core, this refers to crimes that have existed long before the advent of computer technology but has been advanced and amplified by technological developments (e.g., fraud). These are the so-called computer-assisted crimes. The other phrases encompass the crimes that are considered to be made entirely possible by, and are thus dependent upon, technology (Furnell, 2003; Holt & Bossler, 2016; Jewkes & Yar, 2010; Wall, 2007a; Wall 2007b; Yar, 2013). It is recognised, however, that the lines between the two can be blurred and it is difficult to determine how one is to place a certain crime into one or the other. Consider for example the new and fast developing malware called ‘ransomware’; holding something ransom is not a novel act, but rather long-standing, however holding computer files ransom is new and completely dependent on technology. Should this then be defined as a computer-assisted crime or a computer-dependent crime? I would argue, in thread with the classification by SOCTA (2017), that it should be considered as a computer-dependent crime, due to the fact that is, by characterisation malicious software, which would not be able to operate without technology.

In order to make this argument, Wall’s (2007a) transformation test theory has been applied. This test accentuates the relation between the crime and networked technology. In short, it asks what happens to the crime or behaviour if one removes the Internet from the equation (Neal, 2010; Wall, 2007a). There are two binaries in his theory: ‘true’ cybercrime and ‘traditional’ cybercrime. ‘Traditional’ cybercrime are the crimes that have existed long before the Internet was invented, and only expanded and amplified when the Internet was developed (Wall, 2007b: 398).
Examples of ‘traditional’ cybercrimes are violent pornography and stalking (Neal, 2010: 77). ‘True’ cybercrime, on the other hand, is something that has occurred as a result of the Internet; it was developed for the Internet and it will cease to exist if the Internet is removed (Wall, 2007b). Hacking and spamming are some of the crimes considered to be ‘true’ cybercrimes (Neal, 2010; Wall, 2007a; Wall, 2007b). Thus, on the basis of this equation, the ransomware example provided above can be considered to be a true cybercrime and can therefore be categorised as a cyber-dependent crime. As mentioned earlier, it is these types of crimes that are the subject of this study; the section of AlphaBay dealing in true cybercrime tools and services.

1.2.1 Typologies

Hacking and hacking related activities are the most widely discussed types of cybercrime and have to a large extent become synonymous with cybercrime (Yar, 2013: 24). Although it is not an entirely wrong association to make, considering the high newsworthiness of hacking (Furnell, 2010; Holt & Bossler, 2016; Jewkes, 2011), there are still many other types of cybercrime that differ greatly from that of hacking. I do not intend to go into a detailed discussion of the different kinds of offences taking place in cyberspace or the impact these have on society in general, but rather to provide an idea of the scope of cybercrime as a phenomenon and an overview of the types of transgressions that exist. Furthermore, a presentation of the types of cybercrimes that are the focus of this thesis is indispensable.

The information provided in the previous section forms the foundation for understanding the types of deviant acts committed in cyberspace and by use of networked technologies. Under the category of computer-assisted crimes (i.e., not true cybercrime) one finds offences such as fraud, identity theft, piracy, pornography, child pornography, hate crime, and stalking (see Holt & Bossler, 2016; Jewkes, 2011; Jewkes & Yar, 2010; Wall, 2007a; Yar, 2013). Offences such as hacktivism, cyber-warfare and cyberterrorism, which are politically or ideologically motivated offences, are in a kind of grey zone between computer-assisted and computer-dependent crimes. Unfortunately, it is not relevant for this paper to go into a discussion regarding these types of offences, but it is recommended to look at the references listed above for an interesting read.

Computer-dependent crimes (i.e., true cybercrimes) involve offences of hacking in various forms; often including the use of malicious software (e.g., ransomware, Trojans, viruses, worms, keyloggers, spyware), website defacement and ‘spoofing’, gaining unauthorized access
and stealing valuable information, spamming, botnets, and distributed denial of service (DDoS) attacks (Furnell, 2003; Furnell, 2010; Jewkes, 2011; Jewkes & Yar, 2010; Sandywell, 2010; Wall, 2001a). Because the tools used by cybercriminals are developed by those who have collectively become known as ‘hackers’ (Furnell, 2010; Holt & Bossler, 2016; Jewkes, 2011), it is easy to understand that cybercrime often is used synonymously with hacking. This becomes particularly apparent when one considers the fact that though many cybercriminals, and cyberterrorists or hacktivists for that matter, are not hackers, but rather they are ‘users of hacking’ (Jordan, 2008: 97, emphasis not in the original).

1.3 The Darknet

An increasing amount of people have heard about the Darknet and the Deep Web, and the two terms are often, mistakenly, used interchangeably. In short, the Darknet can be explained as ‘any web page that has been concealed to hide in plain sight or reside within a separate, but public layer of the standard internet’ and can only be accessed via additional software (BrightPlanet, 2013: 3; see also Moore & Rid, 2015). The most commonly used software are Tor, I2P and Freenet, with Tor being the largest (Moore & Rid, 2015: 15), which is also used for this study. The Deep Web, on the other hand, is not hidden in the way that the Darknet is. Rather, it distinguishes itself from the Surface Web by not being ‘accessible to link-crawling search engines like Google. […] In layman’s terms, the only way to access the Deep Web is by conducting a search that is within a particular website’ (BrightPlanet, 2013: 2). A common analogy to the Deep Web is that of an iceberg floating in the ocean; the tip of the iceberg that is above the surface is the Surface Web, whilst the huge chunk of ice that is below the surface is the Deep Web. Because of this analogy and the perfect fit of the terms Deep Web and Surface Web, the latter will not be used when referring to the opposite of the Darknet. Rather, this thesis will utilize the term ‘Clearnet’ when referring to that which is not Darknet. The reason for this is two-fold: firstly it is to stay clear of the iceberg analogy for Deep Web and Surface Web, so that there is no doubt that it is the Darknet that is the subject of study here. And secondly, it is because linguistically Darknet and Clearnet sound better together and form an intended binary. In addition, though not of decisive importance, it has been noted that the market actors on the Darknet market AlphaBay also often refer to the Clearnet when speaking of the Internet outside of Darknet.
1.3.1 Tor

As mentioned above one needs additional software in order to access the Darknet, and one of those is the open source browser Tor. The TorBrowser provides access to the TorNetwork, which is where the Darknet domain .onion can be found. The .onion domains cannot be accessed via regular web browsers such as Mozilla Firefox, Internet Explorer, Safari, and Google Chrome, but one can access regular domains like .com or .org from the TorBrowser. In fact, most users of Tor have never utilized the so-called ‘hidden services’ of Tor (i.e., .onion domains), but rather use their browser to surf the Clearnet ‘more securely or more anonymously’ (Moore & Rid, 2015: 16). The TorProject, which runs the TorBrowser, was initially started to give protection to those who needed to stay hidden while conveying or finding information on the Internet, such as for example whistle-blowers, journalists and members of totalitarian regimes (Moore & Rid, 2015; TorProject, 2016). Tor is used by a variety of organisations and agencies as well, ranging from non-governmental organizations, to law enforcement and the U.S. Navy (TorProject, 2016). It anonymises users by bouncing the signal to several different nodes before reaching the target website, which in turn hides the location of the user from both the website itself and from governmental or other authorities’ surveillance (for more in depth description of how it works, see AlQahtani & El-Alfy, 2015; Moore & Rid, 2015; TorProject, 2016). Although the intentions of the TorProject are noble, they are also unfortunately providing an environment for criminal and harmful behaviour to flourish (Holt & Bossler, 2016; Moore & Rid, 2015).

1.4 AlphaBay

AlphaBay was an illegal marketplace operating on the Darknet; it was located on a .onion domain, which is a hidden service on the TorNetwork and could therefore only be accessed via the TorBrowser. It was shut down in July 2017 after international police cooperation efforts managed to seize some of the serves hosting the marketplace, as well as locating and arresting the owner (Europol, 2017; Greenberg, 2017; Statt, 2017). Their main trade was drugs, but they also distributed firearms; stolen credit cards and identity documents; licit software acquired by illicit means; hacking services; and malicious software amongst other things. It was founded by renowned Russian carders in 2014 and quickly rose to be the largest market on the Darknet, following the fall of Silk Road. As mentioned above, the main distribution was drugs, but that is not what this thesis focuses on. In order to identify a specific market culture of cybercrime

---

3 See screenshot 5 in the Appendix
markets, this thesis mainly collected data from the sections of the marketplace and the forum that revolved around malware, hacking, and other cybercrime tools and services. However, general information was also gathered in order to establish the general market culture displayed in the market. This is important to keep in mind when reading the rest of the paper, as most often when I refer to “AlphaBay” I actually mean the section that distributes true cybercrime tools and services. The display of general market culture, of course, is aimed at the entirety of the marketplace.

1.5 Gaps in the Literature

There has been significant change in the aspect of cybercrime, specifically true cybercrime, in that it has gone from being considered as something being committed by the ‘elite’, i.e. professional hackers, to now increasingly being seen as something that can be committed by someone less skilful (Broadhurst et al., 2014; Décary-Hétu & Dupont, 2013; Holt et al., 2012; Ollmann, 2008; Wall, 2001a). This has been made possible by the constant development of malicious software and other cybercrime tools and services, as well as the emerging marketplaces online where the distribution of these products has increased over the past decades (Décary-Hétu & Dupont, 2013; SOCTA, 2017). Criminal forums and marketplaces exist on the Clearnet, Deep Web and Darknet alike, and are used for various means; from asking questions and learning, to recruiting for illegal activities and selling of illegal goods. Several studies have been conducted on markets and forums online such as the distribution of drugs (Bakken, 2015; Bakken et al., unpublished; Hardy & Norgaard, 2016; Lacson & Jones, 2016), sexually explicit materials (Durkin, 1997; Holt et al., 2010; Sharp & Earle, 2003), and cybercrime tools and services (Ablon & Libicki, 2015; Allodi et al., 2015; Décary-Hétu & Dupont, 2013; Holt, 2012; Holt et al., 2016; Radianti, 2010). The latter will be thoroughly discussed in section 2.4 ‘Previous Research’.

Generally, criminological research on cybercrime has been mostly directed towards issues of sexual exploitation of children, drugs, and terrorism. Several academics (Allodi et al., 2015; Choo, 2011; Holt, 2012; Holt & Bossler, 2016; Radianti, 2010) have therefore recommended further studies into the lesser known markets of true cybercrime tools and services. Most existing studies have been conducted on the Clearnet and Deep Web; hence there is a need for more studies on the markets operating on the Darknet. This thesis therefore seeks to fill the gap in the literature on cybercrime markets. In addition, it aims to further enrich the criminological body of research on Darknet markets and other online illegal markets, by opening up the criminological
debate to the economic sociological aspects of these markets. Most of all, it is hoped that this thesis will contribute to the novel discipline of cyber criminology and its quest to understand the causation of cybercrime (Jaishankar, 2007) through introducing the potential of applying rational choice theory and social learning theory to future studies.

1.6 **Outline of the Thesis**

Chapter two presents the theoretical framework and the previous research on online illegal markets. The theoretical framework mainly consists of contributions from economic sociology, namely Aspers (2011) and Beckert and Wehinger (2012), as well as literature on hacker culture. The chapter also briefly discusses the similarities and discrepancies in the theoretical framework and the previous research accumulated for this thesis.

In chapter three, the methodological approach and considerations are presented. The chapter starts with a brief introduction to netnography and grounded theory, along with justifications as to why these methods were considered appropriate for the project at hand. Further, the chapter shows how the researcher located the field and gained access to AlphaBay, and provides detailed description of what type, and how much, data was collected and how it was analysed. The chapter finishes with a consideration of ethical concerns, as well as some limitations to the study.

Chapter four is the first analysis chapter. Here, the researcher explores the structural features of AlphaBay and investigates the formal and informal mechanisms implemented to regulate the marketplace. The notion of coordination problems (Beckert & Wehinger, 2012) is central to this chapter, as well as the elements of general market culture (Aspers, 2011). The chapter starts with looking at the registration process, and takes the reader through all the features and mechanisms that are central to the well-functioning of the market, such as: administration and staff members, payment method, market rules, levels of trust, and feedback.

Chapter five is the second analysis chapter and looks at the influence of hacker culture on the market. This chapter focuses on the social behaviour of market actors and how their norms and beliefs form the specific market culture (Aspers, 2011) of AlphaBay. The chapter starts by looking at members’ appreciation of technological development and finesse, then moves on to their focus on gathering and sharing knowledge and information; importance of skill; outsiders and law enforcement; internal and external reputation; flaming; and masculinity.
Finally, chapter six provides a discussion and conclusion of the previous concepts derived from the analysis. It is here that the examination of general and specific market culture takes place, which shows that specific market culture is not just specific to cybercrime markets. The chapter concludes the findings and discusses their implications, as well as place them in a larger criminological context by briefly discussing their relevance to rational choice theory and social learning theory. Recommendations for future research are also enclosed in this chapter.
2. Literature Review

“There are cultural elements that constitute the background for all social interactions, and those that are similar to many markets and others that are unique to a specific market.”

(Aspers, 2011: 93)

This chapter sets out to present and discuss the theoretical framework for this thesis and provide an overview of the current field of study. It starts off by briefly introducing the academic field of economic sociology, which functions as the main theoretical framework, and the definition of markets within this field. Of particular importance in this study is Aspers’ (2011) distinction between general market culture and specific market culture, and Beckert and Wehinger’s (2012) notion of coordination problems in illegal markets. In addition, an introduction to the intricacies of hacker culture will be made, as well as the concepts and values identified by criminological researchers of hacker culture. It is deemed essential to provide an overview, as well as a limitation, of what constitutes hacker culture, as it is used as an important analytical tool in the analysis for this project.

After the theoretical framework has been thoroughly presented, an overview of the previous research on online illegal markets follows. Their findings and implications are discussed throughout the section, with reference to the theoretical framework where applicable.

The chapter finishes with a summary of what has been presented, along with a brief discussion on some of the similarities and discrepancies identified in the literature accumulated for this study.
2.1 Economic Sociology

Economic sociology has its roots in the works of classical sociologists Max Weber, Karl Marx and Emile Durkheim, with their critique of economic theory’s lack of attention to the social aspects of the economy, and the interaction and relationship between market actors (Granovetter & Swedberg, 2001; Swedberg, 2013). Economic sociology has since been further developed into a ‘new’ or ‘modern’ economic sociology, with Mark Granovetter’s (1985) article on the embeddedness of economic behaviour in interpersonal networks and social actions at the forefront of the development (Fligstein & Dauter, 2007; Granovetter & Swedberg, 2001; Swedberg, 2013). Economic sociology is now a well-established academic field; filled with articles and empirical research using this approach to subjects regarding markets, institutions, consumption, and otherwise (Fligstein & Dauter, 2007; Fligstein & Dioun, 2015). It is clear, and perhaps obvious from the name of the field, that economic sociology is, at its core, mostly concerned about the argument that economic action is social action (Aspers, 2011; Fligstein & Dauter, 2007; Fligstein & Dioun, 2015; Granovetter & Swedberg, 2001; Swedberg, 2013). In other words, everything that happens on a market, for example from the way it was built to the way it works, is socially constructed.

The particular branch of economic sociology that specifically focuses on the sociology of markets is speckled with different approaches to the subject, which makes the definition of a market somewhat difficult. Patrik Aspers (2011) provides a concise definition in his book where he defines a market as ‘a social structure for the exchange of rights in which offers are evaluated and priced, and compete with one another’ (2011: xi). Fligstein and Dauter (2007), on the other hand, provide a more detailed description of what constitutes markets, which also demonstrates ideological differences in neoclassical theory and economic sociology:

“For neoclassical theory, markets simply imply exchange between actors for goods and services. These exchanges are usually thought to be fleeting, with price […] determined by the supply and demand for the commodity. From the point of the sociology of markets, the problem is that this type of exchange already shows a great deal of social structure. Market actors have to find one another. Money has to exist to allow market actors to get bartering nonequivalent goods. Actors have to know what the price is. Underlying all exchange is that both buyers and sellers have faith that they will not be cheated. Such faith often implies informal (i.e., personal knowledge of the buyer or seller) and formal mechanisms (i.e., law) that govern exchange. […] For sociologists, market exchange implies a whole backdrop of social arrangements that economics does not even begin to hint at.’ (2007: 112-113)
Thus, it becomes increasingly apparent that according to economic sociology, and the sociology of markets specifically, that markets are socially constructed and enforced by the use of formal and informal mechanisms. These formal and informal mechanisms play a vital role in the analysis of this paper.

In addition to the social network approach presented above, economic sociologists have had an increasing interest in the importance of culture for markets and market actors (Aspers, 2011; Fligstein & Dauter, 2007; Granovetter & Swedberg, 2001; Sandberg, 2012). Indeed, culture is, to some, considered as an essential part of any equation looking to understand markets as phenomenon, as well as market behaviour (Abolafia, 1998 in Granovetter & Swedberg, 2001; Aspers, 2011; Sandberg, 2012; Zelizer, 1979 in Granovetter & Swedberg, 2001). Hence, market culture serves as the backbone of this thesis. According to Aspers (2011) culture can be understood as the beliefs, norms, tools, rules, and behaviours that are considered appropriate by the market community (2011: 9, 93). Thus, as can be seen in the analysis of this paper, market culture also involves informal cues like ‘what to expect from those in the market, what to talk about and when, and how to do so’ (ibid: 156).

Furthermore, Aspers (2011) also distinguishes between two types of cultures present in markets: a general market culture and a specific market culture (Aspers, 2011; Sandberg, 2012). In short, general market culture refers to elements that span many markets and that are utilized by market actors to create order (Aspers, 2011: 94). Indeed, general market culture spans most, if not all, markets and ‘is made up of ideas concerning what a market is and how market actors normally behave when in the market – for example, when acting as a buyer’ (Aspers, 2009: 8). As an example: the subject of study for this thesis, AlphaBay, and its predecessor as largest Darknet market, SilkRoad, have certain cultural elements in common that will most likely also be found in other Darknet markets. In other words, these general market culture elements are applicable in other markets, and serve as a ‘toolkit’ for market actors (Swidler, 1986; Aspers, 2011: 94). A specific market culture, on the other hand, involves elements that are unique to a specific market (Aspers, 2011: 94). In the examples of elements of specific market cultures in legal markets, Aspers writes that it can include norms and beliefs such as ‘who pays for lunch’ and ‘how people talk, what an office should look like, or [...] what kind of car they should be driving’ (2011: 94).

The notion of a general market culture will be applied in the first analysis chapter of this thesis (chapter four), and will be analysed by applying the coordination problems of illegal markets identified by Beckert and Wehinger (2012) (see section 2.2 below). Subsequently, the concept of a specific market culture is presented in the second analysis chapter (chapter five), and will be
evaluated by applying hacker culture (see section 2.3 below). In addition, the two will be further discussed in the concluding chapter.

2.2 Coordination Problems

In their exploratory article on economic sociology and (offline) illegal markets, Jens Beckert and Frank Wehinger (2012) investigate the functioning of illegal markets and the coordination problems faced by actors operating there. It is not their intention, nor is it mine, to present a general model by which one can determine the functioning of illegal markets, but rather to demonstrate general traits found in these markets (Beckert & Wehinger, 2012: 11). The coordination problems, which are the ‘cornerstones in the study of legal markets’ (Beckert & Wehinger, 2012: 7), are referred to as value, competition, and coordination. Each of these will be presented below.

2.2.1 Value

The first coordination problem presented by Beckert and Wehinger (2012) is that of value. As an introductory description, they write that:

‘The problem of value refers to the assignment of value to a certain category of goods (e.g. cars, wine and travel), and second to the assignment of different values to heterogeneous products within the same market.’ (Beckert & Wehinger, 2012: 12, emphasis in original)

And that the problem of value encountered by market actors ‘are to be found primarily among the difficulties of assessing product qualities in the absence of legally enforceable regulations’ (Beckert & Wehinger, 2012: 13). In other words, because of the illegal nature of these markets, there is no regulating power to ensure that the products traded on these markets meet certain standards of quality (ibid.: 13). Legal markets are subjected to both quality standards and safety regulations administered by the state, the absence of which in illegal market causes what Akerlof (1970) famously characterised as information asymmetry (Beckert & Wehinger, 2012: 13).

Further, they go on to provide examples of mechanisms implemented by actors on illegal markets to tackle this asymmetry of information. Of particular importance in illegal markets operating in the physical world is ‘reputation through personalised networks’ (ibid.: 13). As an example, they draw attention to illegal drug markets, where personalised networks are essential to the perceived quality of a product (Beckert & Wehinger, 2012; see also Sandberg, 2012). In addition, trusted
middlemen work as assurance of quality and guarantors can be to prevent one part from cheating the other (Beckert & Wehinger, 2012: 14). They also argue that the ‘creation of value for a certain class of goods […] is largely irrelevant in illegal markets’ either due to the product being a sincere necessity for the consumer (e.g., organ transplants), or because of the value the product holds on legal markets (ibid.: 12). However, this is not the case when it comes to malicious software and other cybercrime services as these are neither a necessity nor sold on legal markets. Accordingly, the question arises of how actors on Darknet markets dealing in malware and other cybercrime services tackle the problem of value? How is value assessed with no legal comparative market?

2.2.2 Competition

The second coordination problem presented is that of competition. What is central to this issue is presented by Beckert and Wehinger (2012) as the following:

‘To ensure profits, suppliers must create market structures that provide protection from (price) competition. […] The state plays a key role in the market struggles in legal markets by laying down ground rules, for instance in competition law or intellectual property law and by granting subsidies or collecting customs and tariffs (Fligstein, 2001a).’ (Beckert & Wehinger, 2012: 14, emphasis in original)

Obviously, the state and its regulating force is absent from illegal markets and thus market actors must find other means to counter the problem of competition. In their article, Beckert and Wehinger (2012) separate the focus of analysis of competitive problems into two categories: that of firms’ strategies to tackle competition, and the effect intransparency has on illegal markets in the form of ‘inefficient competition’ (ibid.: 15). Since this thesis doesn’t involve corporate firms, the focus here will be on the latter. The intransparency of illegal markets refers both to the difficulties dealers have in terms of advertising goods, and the issues presented to potential customers in terms of comparing price and quality of goods (Beckert & Wehinger, 2012: 16).

According to Arlacchi (1998), the illegal markets of the physical world are limited geographically because the expansions are only local, and the competitive structures are dependent on personalised networks (in Beckert & Wehinger, 2012: 16). Due to this dependency on personalised networks to identify competitors in the market, illegal markets are, according to economic theory, ‘structurally inefficient’ (ibid.: 17). Illegal markets on the Darknet, on the other hand, are global in expansion and not dependent on personalised networks; are they too structurally inefficient?
2.2.3 Cooperation

The third coordination problem explored by Beckert and Wehinger (2012) is cooperation, which at its core can be described as follows:

‘Market actors are confronted with problems of cooperation emerging from the social risks of exchange, notably that of non-fulfilment of contract. These risks arise from the asymmetric distribution of information regarding price, product quality and the possible opportunism of exchange partners in light of incomplete or non-enforceable contracts.’ (Beckert & Wehinger, 2012: 17, emphasis in original).

As indicated by the label, this coordination problem relates more directly to the transactions and relations taking place on illegal markets. Not only is there a lack of protection by the government in a trade, but market actors also risk persecution from the state (ibid.: 22), which means that they must also work against, or at least hide from, the authorities (ibid.: 17). Due to both the lack of enforcement of contract and the uncertainty regarding price and product quality, trust becomes an intrinsic element of illegal markets (ibid.: 17). In terms of organisations and personal networks, then, the smaller the circle the better (ibid.: 18). Furthermore, market actors need to use other mechanisms to enforce cooperation than legal market actors, which can explain the threat, or use, of violence on some illegal markets in the physical world (ibid.: 19). Arguably, trust becomes even more important in online illegal markets, where anonymity is a central component and the use of violence as a mechanism of enforcement is insufficient. This will be explored further in the previous research (section 2.4) and the analysis chapters of this paper.

To summarise, Beckert and Wehinger argue that illegal markets in the physical world mostly develop poorly due to the coordination problems that confronts market actors: ‘valuation is difficult because of the lack of information, competition is deficient and cooperation is risky’ (2012: 21). The question, then, is: is this also the case in the computer underground? How do market actors on Darknet markets tackle these problems of coordination? This will be thoroughly discussed in chapter four.
2.3 Hacker Culture

As mentioned above, this thesis will utilize the existing literature on hacker culture as a tool to investigate the possible influence of hacker culture on the specific market culture of AlphaBay. Thus, a thorough introduction to the main concepts and values of hacker culture is essential. Defining hacker culture is made complex by the fact that there are many different types of hackers. Also, many of those whom academics might place under the umbrella term ‘hacker’ don’t actually consider themselves to be hackers (see e.g., Turgeman-Goldsmith, 2008).

Accordingly, the complexities of hacker culture are imminent; how can one define a culture of which the participants themselves might not identify with? The two binaries of “types” of hackers are those who are referred to as White Hats (‘ethical hackers’) and Black Hats (‘unethical hackers’ or ‘crackers’) (Furnell, 2010; Jordan, 2008; Taylor, 1999; Thomas, 2002; Turgeman-Goldsmith, 2008; Wall, 2001a). However, there are also many shades in-between as members of the community themselves often have difficulties in defining what is ‘ethical’ and what is ‘unethical’ (Furnell, 2010; Holt, 2007). What does seem clear, though, is that any use of hacking and hacker tools for malicious purposes is considered ‘cracking’ or ‘unethical hacking’ (Furnell, 2010; Jordan, 2008; Yar, 2013). The latter of the binary, that is the hackers of malicious intent, are arguably the ones that are present on AlphaBay. Though many would argue that the cultural values, beliefs and norms of the differing types of hackers may vary, there is, unfortunately, not room to speculate or discuss these intricate issues, nor is it necessary considering the focus of this study lies on cybercriminals and not on hackers.

It is important to note that the concept of hacker culture will only be used as a tool in order to understand some of the elements of AlphaBay’s specific market culture (Aspers, 2011). Hence, it is not intended for this paper to analyse a “culture of hackers”, but rather use hacker culture as a means to understand the social behaviour of actors on cybercrime markets. The most seminal and extensive academic contributions on hacker culture arguably comes from Jordan (2008), Taylor (1999), Taylor & Jordan (1998), and Thomas (2002). In addition, Holt (2007) conducted a study on how hacker culture manifests itself both online and in the physical world. In thread with cultural criminology (Ferrell, 1999) and economic sociology (Aspers, 2011), these studies have all looked into the values, beliefs, norms and styles of that which constitutes hacker subculture through qualitative research methods such as interviews and ethnographic observations online and offline (Holt, 2007; Jordan, 2008; Taylor, 1999; Taylor & Jordan, 1998; Thomas, 2002). Hacker culture can be considered what Ferrell (1999) refers to as ‘crime as a culture’, meaning that ‘much of what we label criminal behaviour is at the same time subcultural behaviour’ (1999:
From the research conducted on hackers, hacking, and hacker culture, it is apparent that there are particularly three prominent values of hacker culture: technology, secrecy, and mastery (Holt, 2007). Other elements that have also been identified as central in hacker culture are: membership fluidity, male dominance and masculinity (Cere, 2003; Jordan, 2008; Jordan & Taylor: 1998; Taylor, 1999; Taylor, 2003; Yar, 2013); knowledge, commitment, categorisation and law (Holt, 2007); flaming (Jordan, 2008; Taylor, 1999); language, or spelling (i.e., 1337 also known as ‘leet’ speak) (Jordan, 2008; Thomas, 2002); and peer recognition (Jordan, 2008; Wall, 2001a; Yar, 2013).

2.3.1 Technology

Technology is, perhaps, the most obvious and most important value of hacker culture (Holt, 2007; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002). As a cultural value it refers to the relationship humans have with technological artefacts, which is what hackers and users of hacking techniques actually attack (Jordan, 2008; Wall, 2001a). It is also here that the elements of knowledge and commitment, identified by Holt (2007), are most relevant. Knowledge refers to the willingness to learn and expand ones knowledge of technology, programming, systems, and hardware (Holt, 2007: 182). Through knowledge they gain peer recognition (Jordan, 2008), or status (Holt, 2007). In addition, this willingness, and dedication, also intersects with the element of commitment established by Holt (2007). Although Holt considers knowledge and commitment as two separate entities in his 2007 study, they will be used as elements of the value technology in this thesis. This is mainly due to the fact that knowledge and commitment are intrinsic in hackers’ relationship with technology (Jordan, 2008; Jordan & Taylor, 1998), as will also be demonstrated in the analysis of this thesis. The intersection of commitment towards and knowledge of technology and technological artefacts automatically heightens a person’s level of skill, which is an important aspect of mastery (section 2.3.3 below). In addition, heightened skill level increases one’s reputation and boosts peer recognition, which in turn causes a paradox in regards to the value of secrecy (section 2.3.2 below). Technology, understandably, is the epitome of hacker culture (Taylor, 1999: 27).
2.3.2 Secrecy

Secrecy is a perplexing value of hacker culture. It refers not only to the necessity of keeping identities and acts hidden, but also to the ‘old-school hackers’ contempt for secrecy within companies, and the belief that all information should be free (Jordan, 2008; Taylor, 1999; Thomas, 2002). In more recent times, the focus seems to lie on the secrecy of actions and the need to stay anonymous for safety reasons (Holt, 2007; Taylor, 1999). However, because of the importance of peer recognition, there is also an inherent need to brag about what one can do and has done, which further complicates the element of secrecy (Jordan, 2008: 29-32). Ironically, getting ‘busted’ by law enforcement in the sense that they would notice your actions as a cyber-deviant and put you on a wanted list was often proof of your skill, which would boost your recognition amongst peers (Thomas, 2002: 91). Some members of the hacker community, on the other hand, argue that the most skilled hackers would not be known to the police because nobody should even know they hacked into a system. For some, therefore, stealth is more valued than getting busted in order to gain peer recognition, though more difficult to prove.

However, the subject of law and law enforcement are still highly regarded amongst members of the hacker community (Holt, 2007). Considering the importance of secrecy because of the illicit activities conducted in the community, the fact that they often talk about law and law enforcement is perhaps not surprising. Yet, it does constitute a significant element of the value of secrecy. So much so that even at hacker conventions, specifically DEF CON⁴, there is a game called ‘Spot the Fed’, which arguably functions both as a fun game but also as an awareness campaign reminding people not to spill secrets or sensitive information because you can never know if you can actually trust the person you are talking to (Holt, 2007: 193; Thomas, 2002). This issue of trust bears resonance to that which is highlighted in economic sociology; the problem of cooperation (section 2.2.3 above), which will be further deliberated in the analysis. The game also assists in teaching members of the computer underground to look for specific behaviour that stands out; language or actions that do not belong to the hacker decorum (Holt, 2007: 194). In this sense, the game that is played in the physical world is also applied online, when members of online forums judge others based on how they act and how they phrase themselves (Holt, 2007: 194). This will also be discussed in chapter five.

⁴The largest hacker convention in the United States of America (Holt, 2007: 178) (see also the official website for DEF CON at: https://www.defcon.org/)
2.3.3 Mastery

As with both technology and secrecy, mastery is also considered to be an important and complex value of hacker culture (Holt, 2007; Holt & Bossler, 2016; Thomas, 2002). It is also, according to Holt (2007), the only element present in both online and offline studies of hacker culture (2007: 174). Mastery is understood as both the development towards, and management of, new skills, as well as one’s ability to navigate the physical and social environment (Thomas, 2002: xvi). It is apparent, then, that learning is again considered as a vital component, and demonstrating one’s knowledge of hacking techniques is a way of demonstrating mastery (Holt et al., 2011; Furnell, 2010; Thomas, 2002). In addition, a display of mastery will provide status within the community, for example either as recognition in an online environment or in the physical world by being given a Black Badge at DEF CON (Holt, 2007).

In terms of displaying mastery of the physical and social environment, hacker decorum is essential. One needs to be able to communicate in the correct manner, for example in some instances by using or showing knowledge of so-called ‘leet-speak’ (Jordan, 2008; Thomas, 2002). In addition, using ‘flaming’ in the correct manner can be a show of mastering the social environment, and, as shall be demonstrated in the analysis, if flaming is not done in the proper situation or in the right manner, one loses that attempt of displaying mastery. Identifying mastery on its own is difficult, and to a certain extent near impossible, because it is so tightly intertwined with the other concepts of hacker culture. In order to have a more vivid image of mastery as an element of hacker culture, I propose to use an allegory of ‘craftsmanship’. In a sense, hackers take pride in their developments (Thomas, 2002: 71), perhaps particularly the finesse, sophistication, and elegance of the code (Taylor, 2003; Thomas, 2002). How things are built and coded is of great importance for the element of mastery, if something is messy and easy to crack (if legal programs) or to protect against (if deviant programs) then it is not considered good craftsmanship. These issues will be thoroughly discussed in chapter five.

5 ‘A Black Badge is one of the highest honors that DEF CON can bestow on a person or team in recognition of their overall elite skills or outstanding contribution to the security community’ (Black Badge Policy, DEF CON, https://www.defcon.org/html/links/dc-bb-policy.html)

6 ‘Flaming is a term used to describe the particular vituperative tirades of insults that can result when [a] discussion or disagreement becomes heated.’ (Taylor, 1999: 31, emphasis in original)
2.3.4 Masculinity

Of particular interest regarding masculinity, as I have chosen to term it here, is that in addition to being a cultural value, or norm, in itself, it is also heavily entrenched in many of the other elements of hacker culture presented above. As a whole, the computer underground has been knowingly dominated by men (Cere, 2003; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Taylor, 2003; Thomas, 2002; Yar, 2013), and their cultural values have thus been tainted by masculinity. Thomas (2002) exemplifies the way in which gender is an issue in hacker culture when he explains that:

‘The voice of authority [e.g., in relation to Social Engineering] is a particularly gendered, male voice. […] Technological knowledge is coded as a particular form of masculine and gendered knowledge, and in that sense, the voice of authority, expertise, and mastery is also the voice of masculine authority.’ (2002: 63-64)

Interestingly, male dominance and, consequently, hegemonic masculinity (Connell, 1987), are the only constants that has been coherently present in studies of hacker culture (Taylor, 1999: 33). The reasons for this could be many, and one argument is linked to the societal perceptions of gender typed jobs (Wharton, 2012: 205-206). In fact, the computer industry in general is highly male dominated, which could be because of gendered expectations and opportunities given to girls and boys (Taylor, 1999).

In a more direct relation to hacking, Taylor (1999) found that there was a tendency to differentiate between ‘hard mastery’ and ‘soft mastery’, of which the former is the male approach and the latter is the female approach. Hard mastery is where domination is implemented; forced (Turkle, 1984 in Taylor, 1999: 34; Yar, 2013: 26). Soft mastery is more of a ‘conversation than a monologue’; ‘try this, wait for a response, try something else […]’ (Turkle, 1984 in Taylor, 1999: 34; Yar, 2013: 36). Other factors that might perpetuate male dominance and perhaps discourage females from computer science as a whole, not just the computer underground, can be the ‘male gender bias in the language used in computer science’ and the so-called ‘locker room’ environment in which women feel uncomfortable (Taylor, 1999: 33; Yar, 2013: 36). Misogynistic language is typical and the high frequency of misogyny is considered as a vice of the anonymity provided in online environments (Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999). These issues of masculinity and misogynistic language in particular will be debated further in detail in chapter five, where its presence on AlphaBay is discussed.
2.4 **Previous Research**

Previous research into the workings of the computer underground is substantial, however studies on Darknet markets serve a narrower body of research. Nevertheless, the studies that have been made on the illegal markets on the Clearenrt as well as the Darknet provide a fruitful foundation for this thesis. They include analyses of social behaviour (Radianti, 2010), social structures (Holt, 2012), the role of reputation (Décary-Hétu & Dupont, 2013; Hardy & Norgaard, 2016), self-regulation (Wehinger, 2011), signals of trust (Holt *et al.*, 2016), and regulatory mechanisms (Allodi *et al.*, 2015). In addition, some have explored the online illegal markets from a more general perspective, investigating the ‘landscape and character of these cybercrime black markets’ (Ablon & Libicki, 2015: 143). Most studies utilize data from several markets and/or forums, most of them located on Clearenrt or Deep Web, and only a few of them on the Darknet, whilst others have focused their analysis on one specific market; Silk Road (Bakken, 2015; Bakken *et al.*, unpublished; Hardy & Norgaard, 2016; Lacson & Jones, 2016).

Though the approach to studying illegal markets online varies, they also have common denominators that are highlighted in each of the studies. The most apparent, and to a certain extent also the most obvious, is the issue of trust for participants in illegal markets both online (Allodi *et al.*, 2015; Bakken, 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt, *et al.*, 2016; Radianti, 2010; Wehinger, 2011) and offline (Beckert & Wehinger, 2012; Moeller & Sandberg, 2015; Sandberg, 2012). In regards to the latter, the importance of trust in “traditional” illegal markets has already been discussed, as there is a lack of enforcement of contract (see section 2.2.2). In online illegal markets, the problem of anonymity is the most protruding issue because it makes it easier for dishonest sellers (known as ‘rippers’ or ‘scammers’) to make a profit. This is largely because of the lack of legal action available when such instances occur, as in offline markets (see Sandberg, 2012), and also often due to lack of internal regulation of the marketplace (Allodi *et al.*, 2015; Holt, 2012; Holt, *et al.*, 2016; Wehinger, 2011).

There is consistency in the research in the sense that they have all identified some of the means of which these markets, and consequently the market actors, confront the issue of trustworthiness. It is apparent that the matter is interchangeably tackled from both a structural and social perspective. By this, I mean that the structures of the markets discussed in these studies are designed to limit the issues of trust, and the social environment and behaviour of market actors influence perceptions of trust, and the two of them are often intertwined. For example: The implementation of feedback is a structural feature of the market that is designed to
signal to other market actors whether or not a vendor seems trustworthy (Allodi et al., 2015; Bakken, 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016), and at the same time it functions as a social mechanism to build or dismantle someone’s reputation, which in turn affects the vendor’s perceived trustworthiness (Ablon & Libicki, 2015; Holt, 2012; Holt et al., 2016; Radianti, 2010; Wehinger, 2011). Reputation as a concept in itself has, in fact, also been identified as an immensely important factor of illegal online markets. It can function as a social structure which can be transferred from one market to the other in the computer underground (Radianti, 2010), and it works as a regulating mechanism (e.g. through labels indicating trustworthiness such as ‘newbie’ or ‘hero member’) in markets to sustain honest trade and prevent rippers and scammers (Allodi et al., 2015; Décary-Hétu & Dupont, 2013; Hardy & Norgaard, 2016; Holt et al., 2016; Wehinger, 2011). Reputation is particularly important because it often is easy for honest sellers to gain and conversely problematic for dishonest sellers to garner (Ablon & Libicki, 2015; Allodi et al., 2015; Décary-Hétu & Dupont, 2013; Hardy & Norgaard, 2016).

A second concept that is of central importance in these studies either directly or indirectly is that of regulation. Through the research done for this thesis, it became apparent that regulation is a vital element for an online illegal market to be successful. The evolution of online illegal markets from consisting of loosely connected individuals communicating over IRC (Internet Relay Chat) to forum-based markets is an example of this (Allodi et al., 2015; Wehinger, 2011). Forum based markets provide better opportunities for regulating mechanisms, both formal and informal. The administration often provides a set of rules that members of the community must uphold and if they don’t then there will be some sort of punishment, of which expulsion is the harshest (Allodi et al., 2015; Lacson & Jones, 2016; Wehinger, 2011). In addition to the administration, most markets also seem to have moderators who are in charge of ensuring that those who transgress receive a punishment that aligns with the severity of the transgression. This is considered as a mechanism for regulating the marketplace and ensuring its efficiency and evolvement (Allodi et al., 2015; Wehinger, 2011).

Other mechanisms implemented to regulate these markets are: customer feedback (Allodi et al., 2015; Bakken, 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016); reputation, e.g. in the form of usernames indicating trustworthiness (Allodi et al., 2015; Ablon & Libicki, 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Lacson & Jones, 2016; Radianti, 2010; Wehinger, 2011); payment method, e.g. the use of guarantor programs, escrow services and cryptocurrency (Ablon & Libicki, 2015; Bakken, 2015; Hardy & Norgaard, 2016; Holt et al., 2016; Wehinger, 2011); product validation (Holt, 2012; Holt et al., 2016); reporting routines for frauds
(Wehinger, 2011: 211); and requirements of who gets to join, such as background checks and minimum engagement requirements (Allodi et al., 2015; Lacson & Jones, 2016; Radianti, 2010).

On a general note, the threat of online illegal markets is increasing as these markets become more sophisticated and easier to access (Ablon & Libicki, 2015; Allodi et al., 2015; Radianti, 2010; SOCTA, 2017). In regards to cybercrime markets, it is apparent that the tools and services available today are ready to be used by novices and more experienced cybercriminals alike, meaning that the threshold of skill needed in order to launch an attack has been severely lowered (Ablon & Libicki, 2015; Allodi et al., 2015). The cybercriminals seem to always be a step ahead of the authorities and find new ways of exploiting technological advancements, much because of the so-called ‘digital natives’ who have grown up in a world where the Internet and technology is a natural part of their lives (Ablon & Libicki, 2015). In addition, these types of crimes also receive a lot of media attention where law enforcement agencies often present their techniques for taking down an individual hacker or an online deviant environment (Ablon & Libicki, 2015). This, in turn, provides the cybercriminals insight into how law enforcement operate, which can result in their changing of techniques themselves in order to not get caught. The take down of Silk Road, for example, has impacted other markets to increase their security and to be more vigilant in regards to anonymity (Ablon & Libicki, 2015; Lacson & Jones, 2016). It seems to be an eternal game of cat and mouse, and the best thing we can do is to increase our knowledge of the computer underground in order to keep up with their deviant developments and the markets they use in order to distribute their tools and services.

2.5 Concluding Remarks

From the literary research done for this paper, it is apparent that the field of study is both chaotic and calm at the same time. It is chaotic because the studies done on online illegal markets have many different approaches to their subjects of study, but then it is also calm because a lot of the studies have actually come to the same conclusions through different perspectives. From the section discussing the previous research above, I believe it becomes quite clear that a lot of their findings can be further deliberated by the application of economic sociology. Look, for example, at the implementation of feedback systems found in most market studies where it is argued that it functions as a signal of trust (Allodi et al., 2015; Bakken, 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016), or where it is argued to be a mechanism for establishing reputation (Ablon & Libicki, 2015; Holt, 2012; Holt et al., 2016; Radianti, 2010; Wehinger, 2011). Feedback
systems then can be seen as a mechanism of enforcement to battle the coordination problems faced by market actors, such as value (quality and reputation) and cooperation (trust) (Beckert & Wehinger, 2012). Note that trust is a key component in all aspects of the literature presented above; in online illegal markets, in economic sociology, and also in hacker culture where trust is an essential part of the element of secrecy (section 2.3.2). In addition, reputation is immensely important in both online and offline illegal markets. In online illegal markets it functions as a regulating mechanism through hard earned labels on market actors that are difficult for dishonest sellers to gain (Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2016). In offline illegal markets, on the other hand, reputation is gained through personalised networks and functions as a mechanism of enforcement regarding product quality and value (Beckert & Wehinger, 2012; see also Sandberg, 2012).

Arguably, some of these similarities can be considered as part of a broader specific market culture of online illegal markets. The regulatory mechanisms identified across the online illegal markets are to a certain extent alike, and the mechanisms of punishment are often the same; of which banishment is the harshest. These arguments will be further explored in chapters four and five where the theoretical framework is applied to the primary data of this thesis.

To conclude, then, it is apparent that a lot of the elements of illegal markets online found in the previous research done in this field in many ways complement the coordination problems identified in illegal markets offline. Their concerns are to a certain extent the same; validation of product quality, lack of a regulating authority and enforcement of contracts, and the constant underlying issue of trust. Because of the consistency of these issues, they can be considered as part of the general market culture (Aspers, 2011). However, it is also apparent that although the coordination problems identified by Beckert and Wehinger (2012) are clearly also present on illegal markets online as well as offline, online markets have implemented both formal and informal mechanisms in order to tackle these problems. Particularly forum-based illegal markets arguably tackle coordination problems better because of the fact that they are easier to regulate and often have staff members to enforce the formal rules and mechanisms of that market (Allodi et al., 2015; Holt et al., 2016; Lacson & Jones, 2016; Radianti, 2010). Informal mechanisms such as the feedback systems of many online illegal markets increase the transparency of these markets, arguably making price and quality valuation easier than suggested by Beckert and Wehinger (2012). Though the anonymous environment of illegal markets online makes it easier to scam other members, most markets now operate with a relatively intricate reputation mechanism implemented to encourage honest sellers at the same time as it discourages dishonest sellers, and
thus tackles the problem of cooperation highlighted in illegal markets offline by Beckert and Wehinger (2012). The manner of which general market culture is displayed on AlphaBay will be discussed in chapters four and six, and the specific market culture of cybercrime markets will be discussed in chapters five and six.
3. Methodology

‘How does one get close to the empirical social world and dig deeply into it? This is not a simple matter of just approaching a given area and looking at it. It is a tough job requiring a high order of careful and honest probing, creative yet disciplined imagination, resourcefulness and flexibility in study, pondering over what one is finding, and a constant readiness to test and recast one’s views and images of the area.’

(Blumer, 1969, cited in Corbin & Strauss, 2015: 71)

Considering the nature of the aim and objectives of this thesis, a qualitative research method was considered most appropriate. In a qualitative study, the emphasis lies in the depth of a phenomenon; getting deeply into the data in order to gain a profound understanding of the concepts derived as well as being aware of one’s position in the field and one’s own reactions to the subject under scrutiny (Bryman, 2012; Corbin & Strauss, 2015). Because this thesis sets out to explore structural and cultural features of a marketplace, as well as examine general and specific market culture, a qualitative methodology is deemed best equipped for the task at hand. Hence, I chose to use netnography in combination with grounded theory methodology in order to maintain an open-minded approach to the field and ensure that scientific diligence is sustained.

Grounded theory can be viewed as a guide to conducting qualitative research (Bryman, 2012; Corbin & Strauss, 1990; Corbin & Strauss, 2015; Gobo, 2008), and thus, by combining this methodology with netnography I intend to attain a solid empirical framework. The reason for choosing these two methods is both a practical and personal one. Since I wanted to conduct research online, netnography seemed most appropriate as it is defined by Kozinets (2010) as ‘a specialised form of ethnography adapted to the unique computer-mediated contingencies of today’s social worlds’ (2010: 1). I started the research process with genuine personal and academic curiosity regarding the markets distributing malicious software and other cybercrime services and I sincerely wanted to keep that curiosity thriving throughout the process. Therefore, grounded theory methodology presented itself as an excellent means of sustaining that curiosity and develop it into a scientific enquiry.
This chapter starts off by presenting the research design and data collection process of the project. Further, it moves into the technicalities of the raw data collected, before it presents the means of which the analysis of the data was conducted. The chapter finishes with a detailed presentation of the ethical considerations of this study.

3.1 **Research Design and Data Collection**

Because of the limitations in terms of the scope of the thesis and the time prescribed to conduct the research, the design of the project is a case study, which means that I am looking into one specific market on the Darknet instead of several (Bryman, 2012: 67). In this way, I am ensuring the possibility to explore the structural and cultural features of the market on a much deeper level than would be possible if I had collected data from other markets as well. It also opens up the possibility for examining the specific market culture of the market in greater detail, as well as the display of general market culture. In addition, when limiting the research to only one marketplace I also had the opportunity to properly investigate the administrative functions of the marketplace and thoroughly get to know both its physical and social characteristics.

Throughout the research process I have, to the best of my ability, kept an open mind as to where the data is taking me, as is recommended in both grounded theory (Corbin & Strauss 1990, 2015) and netnography (Kozinets, 2010). The research process has been quite fluid, some might even call it chaotic, as data collection and interpretation of data are intertwined and I have moved back and forth between the market and the forum, as well as in the data collected. This is why keeping a research journal has been so important. Not only has it helped me keep track of the impressions I had as a researcher in the field, but it also serves as a means for me to keep an eye on the decisions I have made throughout the process.

In grounded theory, Corbin and Strauss (2015) suggest that a researcher should finish each data collection session with an analysis in order to see where one needs to probe further in terms of delineating concepts. In this study, after ending a session of data collection, I would go back through the data and get a general idea of possible concepts, however I did not commit to a full analysis of the data. The reason for this is that the data collection had to happen quite rapidly and so there wasn’t time to do a thorough analysis of all the raw data after each session. Instead, I always ended each session with a recommendation to myself as to where I should seek data to probe further into some of the possible concepts discovered in the previous session.
3.1.1 Locating the Field

As discussed previously, markets distributing malicious software exist on the Clearnet as well as the Darknet. Yet, I chose to conduct my research on the Darknet, because I find the idea of the Darknet itself incredibly fascinating, but mostly because there seemed to be less research conducted on this particular part of the Net within criminology. As I set out to explore the Darknet markets I had no idea where to begin, I had no knowledge whatsoever on how to access this part of the Net, nor how to find markets relevant for my project. I therefore started out by reading all kinds of sources on the Clearnet about the Darknet and about the markets and forums that could be found there. Even though this is not so-called technical literature, it was useful for me in order to understand how the Darknet works, how to access it, and how to navigate it. After reading about several different markets on the Darknet, AlphaBay emerged as a suitable candidate for my study as it was considered one of the largest markets with both a lot of products and a high number of participants. At the time, I was not completely certain whether or not AlphaBay actually dealt in malicious software, as most of the conversations on the Clearnet seemed to revolve around drugs, but it was renowned for being a market where you could get practically anything and therefore I decided to at least check it out. It turned out to be a rewarding choice.

3.1.2 Accessing AlphaBay

As mentioned in section 1.3 ‘The Darknet’, in order to access AlphaBay and other sites located on the Darknet, you have to use the open source browser Tor. I therefore started my journey into the dark by downloading the TorBrowser from the TorProject website. I soon learned that AlphaBay is a closed market on the Darknet, which means that you need an invitation link in order to be able to register as a member and gain access to the marketplace. The invitation link is essentially symbolic though, as you can find these links simply by searching the open net, however caution is crucial as these links could be used for phishing instead of being ‘clean’ links to the actual market. I found an invitation link that seemed, according to my relative knowledge and intuition, to be legit and not a phishing site and so copied this link and pasted it into the Tor browser address bar.

---

7 https://www.torproject.org/
8 ‘Using email messages to try to acquire personal information, including banking details, from potential victims.’ (Holt & Bossler, 2016: 206)
The first thing I had to do, of course, was to register as a user. I chose to only fill in the mandatory slots, which was ‘Username’, ‘password’ and a 6 digit ‘PIN-number’. For my username I chose a compilation of completely random letters so that it could not be directly traced back to me. Afterwards, I was advised to write down the mnemonic provided by AlphaBay. This served as an extra security measure in case I (or someone trying to hack my account) could not provide the password and/or PIN-number. If this was to happen and I could not provide the mnemonic, all information connected to the account would be deleted, including all the Bitcoins. The security level is quite high on the market; after the user has logged in, the site scans the users’ security and provides an overview of how secure that particular user account is. I, for one, was recommended to disable Javascript for heightened security. This is easily done in the Tor browser where you can heighten the security, and thus disabling Javascript, by clicking on the Onion in the top left corner (see Figure 1). In addition, on the home page of the market there is a section dedicated to informing/reminding you of your current security level (see Figure 1).

Figure 1: Home page with the security recommendation highlighted in the red box by the author

9 In short, Bitcoin is a cryptocurrency popular on on line illegal markets because of its anonymising features (for more details, see Chandler, 2015)
The forum coupled with the marketplace that has also been used for this study can be found on the navigation bar at the top of the page (see Figure 1). When you click on it, the forum opens in a separate tab automatically so that the user can be on both the market and the forum simultaneously. When I started looking around the forum, I was confused because all the discussion threads were listed as ‘private’ and were displayed as empty, but I quickly realised that I had not been automatically logged in to the forum even though I was logged in to the market. In fact, I had to register as a new user on the forum as well so I decided to apply the same username but a different password than the one I used for the market. Additionally, in order to register as a user of the forum I also had to provide a genuine e-mail address. I chose to use an old e-mail address that I no longer use in case it should get compromised somehow. Once I had successfully registered and logged in I had access to all the discussion threads and I was permitted, like other members, to create new threads, post in those already created and reply to the posts of other members.

Further exploration and details of the structural design of the marketplace will be provided in chapter four, where I analyse the structural features and mechanisms of enforcement; the functionalities of the market and the rules of conduct set by the owner(s).

3.2 The Data

The primary data for this project consists of screenshots taken to document discussion threads on the forum accompanying the AlphaBay market. These were chosen as a means to explore the social and cultural dynamics between the members of the market and how they relate to each other. In addition, I have collected screenshots of vendor profiles to examine the way in which they promote themselves as vendors and what kind of feedback they receive on their products and if (and in that case how) they respond to the feedback and what effect this has on both the market structure and the social dynamics of the market. As a supplement to these screenshots taken with the explicit intent of analysis, I have also collected screenshots of products sold on the market, the lay out of the market and the forum, statistical overviews of the market and forum, and other observationally relevant parts. These screenshots are collected as a means of “general information” about the market and forum, both for my own and the reader’s convenience, in order to gain a coherent picture of how the market and forum is put together. For me, exploring the market and the forum in full and collecting screenshots of the relevant areas was a means to properly get to know the field, which is essential in studies of both
grounded theory and netnography (Corbin & Strauss, 2015; Kozinets, 2010). Furthermore, screenshots are considered as an impeccable way of ensuring enough data to be collected and explored, as online black markets can under certain circumstances and without warning shut down or relocate, and the field would be lost.

I also kept a detailed research journal, which functioned as provisional fieldnotes that complemented the screenshots collected. In the research journal I continuously explained the steps I took when navigating around the market and forum, both in terms of looking at products or discussion threads and statistics or informational content. In this way, I could more easily keep track of where I had been and how I had gotten there, in case I wanted to come back to that place on a later occasion, or if I just needed to know where I found certain information. The research journal ended on a total of 14,411 words (approximately 45 pages in a Microsoft Word document).

### 3.2.1 Primary Data

For the analysis, I collected 717 screenshots from a total of 12 discussion threads, and 316 screenshots from 11 vendor profiles. In addition I have 142 screenshots of statistics and more general information that is relevant for the entirety of the study. In the beginning of my studies on the market I spent quite a lot of time simply figuring out which sales categories (see Figure 2) were relevant to look into in order to find what I was interested in. Under each category there were several sub-categories, which meant that I needed to check several categories for possible points of interest. For example, under the category ‘Guides & Tutorials’ (which had a total of 8613 discussion threads at the start of my data collection) there was a sub-category named ‘Hacking’ where one

![Figure 2: Sales categories](image-url)
could buy guidebooks or tutorials from hackers on how to hack. The most obvious category of relevance for this study was the ‘Software & Malware’ one, which has remarkably less discussion threads than others (a total of 1511 threads at the time). In addition to these two, I also collected data from the categories named ‘Services’ and ‘Security & Hosting’.

The strategy I used when deciding which vendor profiles to use was done by deciding to collect different types of products (e.g., malware, tutorial, botnet, or hacker-for-hire) at different price levels and, subsequently, choose the vendor whom had listed that product. By collecting vendors that sold both expensive and cheap products of different kinds, it was hoped to gain as varied material as possible in order to ensure good qualitative data.

On the forum, I used a similar strategy for data collection as on the marketplace by looking into the sub-sections of each section on the forum (see Figure 3). In choosing which discussion threads to screenshot, I decided to take some that had a lot of comments and replies and recent activity, and some that had less comments and replies. This was in hope of gaining a broader picture of the social structures and cultural dynamics present on the forum. Those threads that had more comments and replies obviously sparked an interest in the members of AlphaBay, and the social dynamics, whether positive or negative, of these interactions formed the basis of my analysis of these threads. In addition, collecting threads that had fewer respondents provided insight into what was not considered important to the community, and the few responses that were there often answered that very question.
3.3 Analysis

The researcher appreciates the detailed work progress described by Corbin & Strauss (2015) for conducting grounded theory research, however when fusing grounded theory with netnography, I applied an even more fluid progression than is established by the authors. Instead of specifically sitting down and doing a detailed analysis of the data collected during a specific session, general analysis was conducted continuously as I collected data. The instant a possible concept appeared, the data collection was taken in the direction to explore this further. It is also important to bear in mind that I was not dependent upon interviews or observational episodes to prepare for prior to each session; rather, I had the freedom to go back and forth between data as new concepts were delineated to check for continuity, dimensions and properties of these concepts during more in-depth analysis.
Once all the data had been gathered, a more in-depth analysis began. First, I decided to organise the screenshots into Microsoft Word documents, separating them with headlines determining their belonging (e.g., “Discussion Thread: The Malware on AlphaBay”). However, during the organising of the screenshots into the documents I realised that this would be an extremely tedious and time-consuming way of coding, considering the amount of primary data I had gathered. Therefore, I instead decided to code the data directly into separate word documents for each code (e.g., one document for “secrecy”, another document for “trust”, et cetera), which would make navigating through the codes easier. I separated the coding process into two parts: one for the coding of the marketplace data (e.g., vendor profiles), and one for the forum discussion threads. This was done for two reasons: first, because it seemed appropriate to distinguish between data from the marketplace and data from the forum; and second, because data from the marketplace was mainly used in the first analysis chapter (i.e., chapter four) and data from the forum was mainly used in the second analysis chapter (i.e., chapter five). This does not mean that I excluded one in favour of the other in the respective analysis chapters; both datasets were utilized in both analysis chapters, but to varying degrees.

Every single discussion thread and vendor profile collected were comprehensively examined and coded accordingly. Some of the codes were derived from the literature on economic sociology and hacker culture, and some were derived from the data. In chapters four and five, I have used the codes and categories identified in the data in combination with the theoretical framework in order to answer the overall aim and the first two objectives of this thesis. In addition, the elements of general market culture and specific market culture that are identified throughout those two chapters is further discussed in chapter six in order to answer the third objective of the study.

3.4 **Ethical Considerations**

There are several ethical considerations to adhere to in this study, and I have done my utmost to uphold sound ethical standards. I have sought guidance in both the methodologies I have utilized, in previous work done in the field, and in the National Committee for Research Ethics in the Social Sciences and the Humanities’ (NESH) (2006) ‘Guidelines for Research Ethics’ and their more specific 2014 guidelines for research conducted on the Internet.
3.4.1 Public versus Private Space

It is quite apparent that doing research on the Internet introduces complex ethical issues that are similar but also distinct from the ones in the physical world (Bryman, 2012; Corbin & Strauss, 2015; Holt & Bossler, 2016; Kozinets, 2010; Markham, 2011). Perhaps the most obvious issue is the debate on whether the Internet should be regarded as a ‘public’ or a ‘private’ space (Bryman, 2012; DiMarco & DiMarco, 2003; Holt & Bossler, 2016; Kozinets, 2010). This is problematic because it triggers the question on how the researcher is to announce their presence. If the space is considered private, then the researcher is ethically bound to disclose their purpose and obtain informed consent from the participants (Bryman, 2012; NESH, 2014; Kozinets, 2010). However, if the space is considered public, then the researcher can gather data without explicit consent from the participants as long as they do not disclose personal and private information in their report (Bryman, 2012; NESH, 2014; Kozinets, 2010). The question I had to reflect on in this thesis, therefore, was whether AlphaBay was to be treated as a public or a private space. I decided to treat it as a public space, and the reasons for this are copious. To a certain extent, AlphaBay could be considered a private space because it is hidden (i.e., on the Darknet) and it is closed (you have to register as a member to view and add content). However, because of the nature of the marketplace that encourages an open market where anyone can get hold of what they need, I argue that it can be considered a public space. It allows anyone to register as a buyer and you are allowed to use the forum to discuss exactly what you want to discuss. In addition, they (i.e., the administration of AlphaBay) have posted several tips and guidelines for their users of dos and don’ts precisely because of the relative openness of the marketplace and thus the awareness that “someone may be watching”. Even though they are mainly referring to law enforcement, it could also be considered as a warning by the administration that anything you post on the market or forum is subject to scrutiny by others, including a researcher such as myself.

Another justification for treating the market as a public space, and not announcing my presence, is the risk that the site could be shut down or moved to a different domain by the administration. AlphaBay, as a “professional” online illegal market, is dependent on keeping their site up and running, and would probably not risk having an “outsider” lurk around their premises. Therefore, I could risk having my user profile deleted and banned, making access difficult. On AlphaBay, there are no rules against “lurkers”, though, and anyone logged on to the forum can see that I am also there although I am not posting or commenting anything. Indeed, I
saw many other users that were simply there without posting or commenting\textsuperscript{10}. As long as AlphaBay has not specifically said that no one is allowed to use the information posted on the market or forum for other purposes than their own, which they haven’t done, anyone can lurk around their sites collecting the information they please (Bryman, 2012: 679).

### 3.4.2 Protection of Participants

When conducting research online, it is important to bear in mind that usernames, pseudonyms and direct quotes can be found by a simple search in an online search engine (e.g., Google) (Bryman, 2012; Corbin & Strauss, 2015; Kozinets, 2012). One should therefore consider whether or not it is necessary to re-write a statement or a segment of data before presenting it in a report. This thesis, however, utilises direct quotes from discussion threads and feedback comments. Due to the fact that AlphaBay is located on the Darknet, it cannot be found by simply inserting the quote in a search engine on the Clearnet. However, several authors (Bryman, 2012; Corbin & Strauss, 2015; Kozinets, NESH, 2014) have stressed the importance of treating pseudonyms on the Internet on the same level as one would treat a person’s actual name. Though it could be argued that the anonymous nature of AlphaBay, the steps taken by its denizens to protect their identity, and the fact that it is un-searchable on the Clearnet, I decided to censor all usernames from the screenshots and not use any names in the quotes or in my own descriptions of situations. This is done both to protect the participants, and to protect myself; if any of them were to read the thesis and see that I had published their usernames, I might be finding myself with an infected laptop shortly after. I admit that it might be a slightly paranoid reason, but a reason nonetheless.

### 3.4.4 Limitations

Beneficial to all observational studies is the opportunity to interview the participants in order to record their opinion of the situation (Corbin & Strauss, 2015). Even though I have done my best to keep my mind open, the fact remains that the interpretations of my observations on AlphaBay are my own; based on the theoretical framework and the previous research done on online illegal markets. The denizens of AlphaBay themselves have not had the opportunity to comment upon their perception of the community, which could either underscore my findings further, or perhaps take the findings in a different direction than this thesis did. However, the

\textsuperscript{10} These were labelled as «ghosts», see section 4.2
issue of recruiting possible participants remains the same as to why I did not disclose my presence on the marketplace; it would likely interrupt my access to the field, unless I purposely singled out members to ask them to join the study. Albeit this approach could lead me into a problematic situation, as I would not be able to know the ties that member had to AlphaBay, or their roots in the physical world. Again, the question of my own safety is also raised; considering AlphaBay is an openly illegal market, the motivations of the participants maybe predatory and thus the safety of the researcher might be compromised (DiMarco & DiMarco, 2003: 169).

Collecting data online can be problematic, especially in such a highly anonymous environment such as AlphaBay, because you never actually know who the people behind the usernames are (DiMarco & DiMarco, 2003; Kozinets, 2010); there might be more than one person operating with the same user account, or there might be one person operating with several user accounts. This is something that has been on the back of my mind throughout the research process, and it turned out to be an issue the participants of AlphaBay were also very aware of for various reasons11.

Furthermore, the thesis is arguably limited in its study of the specific market culture of cybercrime markets. It would have been beneficial to collect data from multiple cybercrime markets in order to crosscheck and validate the findings. However, because of the scope of this project, there was not sufficient time to go deeply into several Darknet markets in order to answer all of the objectives. I have, instead, kept a critical approach to my findings, crosschecking them with previous research to ensure due diligence.

11 See section 4.6 about feedback and section 5.4 about outsiders.
4. Structural Features and Mechanisms of Enforcement

“We can now officially say that no market has a feature that we don’t.”

(AlphaBay Administrator, September 9th 2014)

The following chapter will present, explain and discuss the structural features of the Darknet market AlphaBay and the mechanisms implemented to ensure a well-functioning marketplace. The goal is to gain a deeper understanding of how the market works and why these procedures are successful or unsuccessful in their application. It is hoped that this chapter will provide a vivid image of the sophistication that lies in the operation of the market, as well as the processes involved in establishing trust and the mechanisms employed to tackle coordination problems (Beckert & Wehinger, 2012). I will argue that some of the findings of this analysis can be considered as part of the general market culture for markets operating both online and offline, an argument that will be justified throughout the chapter.

The chapter is presented in the manner of which I experienced the marketplace, starting with the registration process and the first impressions of the market. It then moves on to talk about the discussion forum and staff members and their respective roles before going into a detailed exploration of the market rules and the punishment mechanisms accommodating said rules. Further is the presentation of the payment method employed. Afterwards, the paper moves on to discuss the implementation of Vendor Levels and Trust Levels and their importance for the efficient operation of the market. The chapter finishes with an in-depth analysis of the feedback system of the market and concluding remarks.
4.1 Becoming a Member

As mentioned in previous chapters, becoming a member of AlphaBay was fairly easy. There were no ‘background checks’ (see Allodi et al., 2016) made in order to be allowed to sign up; anyone can register. Although it is worth noting that it does take a certain amount of determination in order to find out how and where you sign-up, you will not stumble upon the registration page for AlphaBay by accident. During the registration process I was required to create a username, a password, and a 6 digit PIN number. These were the only mandatory slots I had to fill out; the rest, like for example PGP\(^\text{12}\), were optional even though they were recommended. The username and password was utilized for logging in to the market, whilst the PIN number was used for verifying transactions. After all the information had been filled in, I was given a mnemonic that was automatically generated and is individual to each user, which they advise you to write down. The mnemonic will only be asked for if a user is unable to remember his PIN number and/or password; if they fail to provide the mnemonic all information on the account will reset, which could result in the loss of any Bitcoins located on the account. This was done to secure user accounts from being hacked and subsequently stolen from. Some might also argue that the administration could take advantage of this measure and close down accounts and take the Bitcoins themselves\(^\text{13}\).

After the registration was completed, I was taken to the ‘Home page’ of the market (see Figure 4), which displayed the profile on the left hand side as well as in the top right corner with a brief overview of username and current balance in BTC (Bitcoin). In the middle of the page was the section of “featured listings” which presented some of the listings on the marketplace. Some of the details of the user profile were summarised on the left hand side and, as Figure 1 shows, all new members were placed in Trust Level 1 (trust levels will be discussed in section 4.5). After registering, it became apparent quite quickly that the focus on user security is high. When I was first taken to the Home page, there was a warning sign at the top of the page advising me to disable Javascript for heightened protection (see Figure 4). In addition, the administration reminded the users to not give out any personal information in form of name or a Clearnet website than can be linked to them in their profiles on AlphaBay.

---

\(^{12}\) An encryption key for messages

\(^{13}\) This is known as an exit-scam
Figure 4: AlphaBay Home Page

The inherent anonymous nature of AlphaBay and the high focus on security were some of the mechanisms identified that ensured the successful operation of the market. Yet, anonymity was also what made AlphaBay vulnerable; trust is essential for a market to be successful (Bakken, 2015; Beckert & Wehinger, 2012; Granovetter & Swedberg, 2001; Hardy & Norgaard, 2016; Holt et al., 2016; Moeller & Sandberg, 2015; Wehinger, 2011), and establishing trust in an anonymous environment is a demanding process (Allodi et al., 2016; Holt, 2012; Holt et al., 2016; Radianti, 2010).

In a legal market, it doesn’t matter if you don’t know who you are dealing with because you are protected by laws laid down by the state that will interfere and ensure the safety of your investments (Beckert & Wehinger, 2012). In an illegal market in the physical world, secrecy is deemed more important than anonymity, and knowing the person you are dealing with is considered the greatest element of trust (Beckert & Wehinger, 2012; Moeller & Sandberg, 2016; Moeller & Sandberg, 2015; Sandberg, 2012). The traditional illegal market to a certain extent
consists of personalised networks (Beckert & Wehinger, 2012; Sandberg, 2012) or organised crime groups (SOCTA, 2017). On the Darknet it is, strictly speaking, impossible to know who you are in contact with. There may be more than one user having access to a user account, or one user with several accounts, and thus when you are in contact with that user you do not know which of the persons you are actually talking to (as exemplified in Figure 13 in section 4.6, where one user was accused of having 7 different accounts).

4.2 The Forum and the AlphaBay Staff

As displayed in Figure 1 above, there was a navigation bar at the top of the page where one could navigate to different parts of the marketplace at ones convenience; for example Support, Balance, or Forums. It was here one could access the discussion forum that was coupled with the marketplace. The discussion forum was a space where the staff published announcements about the market, vendors promoted their listings, and members of the market could review market listings or vendors, as well as ask questions or start threads asking for advice or how to learn certain skills (this will be discussed in more detail in the next chapter).

One could get on the forum without actually signing in, but then one could only see the discussion headings and not the actual posts and replies. The forum was very transparent in terms of who was online and what they were doing; you could go to the ‘members’ section and see who was online at the same time as you and view their recent activity (i.e., which part of the forum they visited last). On the forum members were also placed within a category depending on how long they had been a member and how much they had participated as a member of the forum. The lowest category was called *ghost*, and sequentially the categories were: *new member*, *member*, and *active member*. In addition to these, there was also the administrative staff whose categorization was as follows: *AlphaBay PR, junior moderator, senior moderator, tech support, security administrator*, and *administrator/owner*. Furthermore, there were also other groups of staff getting paid to do certain jobs; for example, “ScamWatch”\(^{14}\) helped the administration with scam reports and removing scammers and spammers from the marketplace and forum; “Notarius”\(^{15}\) staff that were employed to help the administration with handling reported disputes between buyers and

---

\(^{14}\) See Screenshot 1 in the appendix

\(^{15}\) See screenshot 2 in the appendix
sellers; and “GRB”\(^{16}\) (Guide Review Boards) staff tasked with quality checking guides that were for sale on the marketplace to ensure best products for potential buyers.

The administration and other staff members seemed to be sorted into quite an ordinary hierarchal system where the employees had less power to punish and regulate than the administration. Those who were hired as staff could only report members who should be banned to the administration instead of executing the punishment themselves. Therefore, the administration were the only ones who had authority over the mechanism of punishment. The administration on its own also seemed to be divided into a hierarchal system: the PR member’s job, for example, was to answer questions on Clearnet forums and not much else. In contrast, the Administrator and their “right hand” (i.e., the Security Administrator) held a lot more operative responsibility both in terms of the practical running of the sites, the moderating of other staff members, and ensuring the members of AlphaBay were kept up to date on announcements and other important messages (e.g., tips on how to not get busted by law enforcement\(^{17}\)).

The number of members employed as administration or staff members on AlphaBay is arguably a way of handling some of the problems of coordination identified by Beckert & Wehinger (2012). It is clear that this form of regulation and security for the members is an effort to reduce the risk of exchange that is so prevalent in illegal markets (Beckert & Wehinger, 2012). The problem of value and the subsequent problem of quality validation is tackled, at least in regards to guides, by having a designated team to do exactly that: quality check the guides in order to ensure only proper guides are listed. This product quality assurance is also identified as one of the three mechanisms integral in the normative order of trust identified by Holt (2012). Similarly, Holt et al. (2016) also found that having moderators and administrators review your product functioned as a signal of trust, which can be considered as diminishing the risk of exchange and a way to validate its quality (Beckert & Wehinger, 2012).

### 4.3 Payment method

Due to the anonymous reality of Darknet markets, and other online illegal markets, there has to be measures put in place in order to prevent people from scamming each other (Ablon & Libicki, 2015; Holt et al., 2016; Wehinger, 2011). The AlphaBay market, as many other online illegal and legal markets, utilized an escrow system for the transaction of money (Bakken, 2015;  

\(^{16}\) See screenshot 3 in the appendix  

\(^{17}\) See screenshot 4 in the appendix
Bakken et al., unpublished; Lacson & Jones, 2016; Wehinger, 2011). This is done to secure both the buyer and the seller from risks of exchange (Beckert & Wehinger, 2012); if a buyer pays for a product before receiving it, they might not receive it at all if there are no mechanisms put in place to ensure a fair trade. This can also affect the seller, of course; if he sends a product without receiving payment, he may never get the money he earned. The escrow system therefore operated as a ‘safe keeper’ of funds until both parties were satisfied with the trade and had kept their end of the contract. When a buyer placed an order, they put forth a payment, which was held by the escrow system instead of being sent directly to the seller. The seller can see that the money were on the escrow system and therefore knew that the money would be released to them after they had completed their part of the deal and the buyer had received their products. The buyer then finalises the sale, and the money are released to the seller.

The administration made strong warnings not to “finalise early” and not to finalise before the purchased product has been delivered, as discussed in section 4.4. The escrow system worked as an enforcement to keep both buyers and sellers safe from dishonest individuals, just as guarantors are in other markets (Beckert & Wehinger, 2013; Holt, 2012; Wehinger, 2011). As the AlphaBay administration themselves put it, in the absence of legal recourse, if one releases the funds to the seller “there is nothing else we can do” (see Figure 5 below).

One of the major risks of exchange in markets, perhaps especially on illegal markets, lies in the payment method (Beckert & Wehinger, 2013; Hardy & Norgaard, 2016). Therefore, the utilisation of escrow suggests that AlphaBay is battling this coordination problem by implementing a mechanism to ensure fair trade and heightened trust between individuals (Beckert & Wehinger, 2013; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Wehinger, 2011). As it has been noted above, this feature is by no means exclusive to AlphaBay, but that doesn’t render it any less important. In fact, the implementation of a system applied in other known markets shows that this can be considered to be an element of the general market culture. Indeed, payment methods and the perceived security surrounding payment methods is part of everyday life of consumer societies.
4.4 Market Rules

As mentioned previously, the administration utilized the discussion forum for announcements. This was also where they published the rules for trading and the rules for behaviour (Figure 5).

**The following rules apply for trading:**
- When you place an order, you can’t cancel it, unless you come to a mutual agreement with the seller.
- When the order is finalized, the funds are released to the vendor and there is nothing else we can do.
- Do not send funds outside of Escrow. If you do so, it is entirely at your own risk.
- Do not finalize the order if you did not receive the product, no matter what the vendor says.
- Anything related to prostitution, child pornography, and murder / assassination is prohibited on the marketplace.
- Orders that are not marked as shipped within 72 hours are automatically declined and refunded.

**The following rules apply for behavior:**
- Using abusive language or behavior will result in a warning. Accumulation can lead to a ban.
- Any dox threat results in an immediate ban.
- Any kind of malware which targets Russian citizens or citizens of any other country from SNG ([URL](https://en.wikipedia.org/wiki/Commonwealth_of_Independent_States) is not allowed. Sale of any financial information of Russian citizens or citizens of any other country from SNG is not allowed. This will result in immediate ban.

The implementation of rules was part of the regulating mechanism used to ensure not only fair and secure trade, but also in order to accommodate the denizens of the AlphaBay community (in that they are claiming to not tolerate abusive language or harmful information about Russian citizens). The fact that members were not allowed to distribute information or cybercrime tools that could harm Russian citizens can be considered both as a security precaution to ensure that the Russian government or law enforcement would not catch interest in the market, or as a display of nationalism since the founders of AlphaBay were renowned Russian carders. Also considering that a section of AlphaBay was entirely in Russian language, and that the ‘Administrator’ account had a signature in both English and Russian, it seems plausible to assume that the site had strong ties to Russia and therefore did not wish any harm towards its citizens or attention from its authorities. In addition, the rules also restrict the distribution of certain goods, mainly those relating directly to human bodily harm (e.g., murder). This could be considered as a means to keep law enforcement relatively uninterested in their marketplace, as these types of crimes are highly prioritised by law enforcement both nationally and globally. Thus, by limiting members’ choice to promote these goods on the market, they attempted to limit unwanted attention towards their market in order to run a structurally efficient and well-functioning marketplace.

---

18 See screenshot 5 in the appendix
19 See screenshot 6 in the appendix
The rules for trading listed above were mainly aimed at the members who were looking to buy, not to sell. The vendors on the market had been introduced to the rules of trading from the sellers’ end of the contract once they signed up to becoming a vendor (see Figure 6).

Vendor Account

Here you can activate your vendor account. Take time to read the vendor rules before, check the box, and click the button. After that, you will be able to create listings and start selling here. Be careful to acknowledge the rules, as breaches them may result in account suspension.

#1: FE (Finalize Early) is not permitted unless you get explicit permission later. You will get banned without refund if you ask for FE without permission.

#2: Digital orders auto-finalize after 48 hours, and physical orders auto-finalize after 14 days.

#3: If you get too many scam reports, we may revoke your vendor account at any time.

#4: There is a USD $200 vendor bond (0.0001 BTC at the current rate), refundable upon closure of account if in good standing.

#5: All sellers must have a PGP key in their profile before starting to sell.

#6: Prostitution, child porn, and murder services are not permitted. Personal information about Russian citizens is also prohibited.

#7: Any dox threat will result in an immediate ban.

#8: Two-factor authentication (2FA) is mandatory for all vendors and will be automatically activated when you become a vendor.

I have read and accept the rules mentioned above.

Become A Vendor

It became apparent that most of the rules for trading were the same, whether you were looking to buy or sell. However, there were some additional requirements in order to open a vendor account. Anyone could open a vendor account; there were no background checks or requirements of participation/length of membership in order to be qualified to become a vendor. The fact that they took a “deposit” of 200 USD, which they stated would be refunded if one wished to close the vendor account, shows that they were encouraging honest behaviour and fair trade from those who opened vendor accounts. If an account was revoked because of scamming, or other rule breaking, the money would obviously not be refunded and the user would lose 200 USD, which, for many, is no small amount of money. Arguably, by requiring such a high sum for a deposit, they might have moderated those who looked towards opening a vendor account simply for the purpose of scamming.

If a scammer were to weigh the risks and benefits of opening an account in order to scam other members, they would have to be certain that they could make more money than they paid to open the account, or else it would not be a profitable scam. Indeed, according to Wehinger (2011), having vendors pay a fee for a vendor account functions as a mechanism of self-regulation (2011: 211).

In addition to the market rules, there were also rules for posting in the discussion forum (see Figure 7).
The posting rules varied from annoying details (i.e. writing in caps lock) to ensuring buyer security by warning members not to initiate transactions outside escrow. The latter could also be considered as a means for the owners of AlphaBay to ensure profits on their own behalf, considering they got 3.5% in commission fees for all transactions. The consequence for breaking these rules also varied in relation to the perceived seriousness of the offence (according to the administration).

The mechanisms of punishment implemented to enforce the rules (i.e., regulation mechanism) were numerous; accounts could be frozen, listings or forum threads could be removed, and users could be banned from the marketplace all together (and consequently lose all their Bitcoins). These were punishments that only the administration could execute, and were the worst consequences of unwanted behaviour registered on AlphaBay. The administration then held the executive power to punish members and can therefore be considered as a regulating force present to ensure a well-functioning market (Allodi et al., 2016; Wehinger, 2011).

Banishment was on its own considered as a severe form of punishment, although on AlphaBay it also had its flaws; they did not operate with background checks or minimum requirements of posting or engaging (see Allodi et al., 2016; Lacson & Jones, 2016; Radianti, 2010). Hence, if a user was banned, there would be nothing to stop them from simply opening a new account and continue their damaging behaviour.

Because AlphaBay was a market that was open to anyone who wished to join, this is a consequence they were willing to endure. Earlier studies have already established that fake accounts can be frequent and difficult to police (Allodi, et al., 2015; Holt et al., 2016). On AlphaBay, claims of so-called fake members having up to 7 accounts to cause harm to other market actors exemplify the extent to which some people would go (see Figure 13 in section 4.6). As long as AlphaBay, or any other online illegal market, continues to operate as a relatively open marketplace, then these problems will persist. Indeed, this was something even the owner(s) of
AlphaBay recognised when they said: “[...] buyers can simply make a new account and start fresh. There will unfortunately always be problematic buyers”.

Members did, however, have an alternative punishment mechanism they were equipped to enforce themselves; namely “Blacklisting”. If one came across a fellow member of the community whom one did not wish to have any contact with whatsoever, and did not want that individual to have access to any of one’s information (meaning both profile and listings), then one could choose to put them on a Blacklist. This is what I consider as the members’ “private ban”, which ensured that that particular member would not be able to place any orders or see any new listings that one has made (see Figure 8). This tool was a clever way for the administration to give community members some agency in the regulation of the market.

The Blacklist was, however, a private protection mechanism and was not publicly visible to other members. In other words, even though a buyer was blacklisted by one vendor, they could still place orders with other vendors without them knowing that they had been considered as a potential risk.

Sellers and buyers did have other alternative actions to take if someone treated them unfairly. If there was a problem with a transaction and the two parties could not agree on a solution the transaction could be disputed. The case would then be handled by a member employed by the administration (i.e., notarius), and the details of the contract would be scrutinised and the notarius would then contribute to resolving the issue. Most times the disagreement was settled by either having the seller refund or reshipe a product, or the buyer having to pay the seller if this had not been done. If a dispute was very complicated and the parties were difficult and not cooperating with each other or the notarius, the case would be handed over to the administration, which held more authority than the notarius. Similar ways of handling disputes between buyers and sellers have also been identified on other online illegal markets (see Allodi et al., 2015; Wehinger, 2011), and is clearly a way for market actors to tackle the problem of cooperation (Beckert & Wehinger, 2011). It also bears resonance to the interference of state or laws of regulation in legal markets, which suggest that this regulating mechanism is part of the general market culture.
Similarly, a community member could file a scam report if they got scammed, which would also be handled by other members employed by the AlphaBay administration. The so-called ScamWatch team would look at the filed report and start gathering evidence in order to make a decision on whether the accused scammer was indeed a scammer and to which extent the member should be punished. The ScamWatch held some authority in the sense that they could order a member to refund the money lost to the victim of the scam, and also to remove people from forum threads if they were spamming or causing disorder. If they found that the scammer needed to be banned from the marketplace, they had to give the report with all the evidence and their recommended action to the administration, who, again, were the only ones with the authority to ban someone. This system for scam reporting is a clear regulating mechanism (Wehinger, 2011) and has also been found in a similar degree in other markets (see e.g., Allodi et al., 2015). It clearly tackles some of the problems of cooperation identified by Beckert and Wehinger (2012) by helping market actors in the absence of legal recourse.

In the physical world, illegal markets often use violence or the threat of violence in order to handle problems of cooperation like those presented above (Beckert & Wehinger, 2013; Moeller & Sandberg, 2016; Sandberg, 2012). Online illegal markets, due to the lack of physical contact and the global anonymous environment in which they operate, are on the other hand dependent upon other means of enforcement. The different levels of punishment described above are designed for this purpose; they are the forces used to regulate the market in absence of governmental regulation and legal recourse (Allodi et al., 2016; Beckert & Wehinger, 2013; Wehinger, 2011). The fact that they had employed members in certain roles to keep the regulation of the marketplace as efficient as possible shows that they strove to run a well-functioning and sophisticated marketplace that could be accessed and used by anyone. Several other illegal online markets have also had designated staff to assist the administration in running the marketplace (see Allodi et al., 2015; Wehinger, 2011). In addition, the implementation of rules and mechanisms of punishment has also been found previously to be an efficient way of regulating an online marketplace (Allodi et al., 2015; Radianti, 2010; Wehinger, 2011). In lack of enforcement of contract from the state and legal recourse (Ablon & Libicki, 2015; Allodi et al., 2015; Beckert & Wehinger, 2012; Wehinger, 2011), these rules and punishments function as a means to tackle the social risks of exchange and cooperation problems (Beckert & Wehinger, 2012).

Being part of the regulating mechanism, market rules and punishments are an imitation of the general market culture. Remember that culture here is about behaviour (Aspers, 2011), and
these rules are implemented to govern market behaviour. They are similar to the role of the state, and its regulating force, in legal markets. Since this has been found in both my data and previous research (Allodi et al., 2015; Lacson & Jones, 2016; Radianti, 2010; Wehinger, 2011), I am confident that if one were to study other online illegal markets trading in illegal goods and services, one would find similar rules and punishments in order to regulate the marketplace.

4.5 Levels of Trust

On AlphaBay, they developed an intricate system in order to best assist members to determine the trustworthiness of a potential trading partner. They used two separate systems: ‘Vendor Levels’ and ‘Trust Levels’. The Vendor levels were a mechanism to ensure safety for buyers when trading with a vendor: the levels indicated the trustworthiness of a vendor through the calculation of how many sales had been made, how much money had been earned, and what percentage of positive feedback the vendor had received (see Figure 9).

We are introducing vendor levels. This was asked by the community, therefore we bring it to you. This will encourage vendors to reach higher levels.

The level will be displayed on listing pages and on the user’s profile page, and go as follow:

Level 1: Anything under
Level 2: 100 sales, $1,000 volume, 95% positive feedback
Level 3: 300 sales, $4,000 volume, 95% positive feedback
Level 4: 500 sales, $10,000 volume, 95% positive feedback
Level 5: 700 sales, $25,000 volume, 95% positive feedback
Level 6: 600 sales, $75,000 volume, 95% positive feedback
Level 7: 900 sales, $150,000 volume, 95% positive feedback
Level 8: 1,200 sales, $450,000 volume, 95% positive feedback
Level 9: 2,500 sales, $1,000,000 volume, 95% positive feedback
Level 10: 3,000 sales, $2,500,000 volume, 95% positive feedback

Many vendors already reached the levels and, also, lower commission fees. This should also be used as an estimate of a seller’s trustworthiness.

Vendors will also see their commission fees lower by 0.5% for each $20,000 worth of transactions. The fee is currently 3.5% but will decrease down to 3.5% with the correct trading volume.

Figure 9: Vendor Levels

However, it also became apparent through the description of the vendor levels made by the administrator that these levels were not only for the benefit of the buyer; they also benefitted the seller. In order to reach higher levels, they had to sell a certain amount of products as well as having certain revenues from sales. The benefit of reaching higher levels was that it increased their reputation as a vendor, which heightened their trustworthiness, which in turn increased sales (see also Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2016; Holt et al., 2016; Radianti, 2010; Wehinger, 2011). In addition; the more money a vendor made, the less commission fee they would have to pay to the AlphaBay owners. In other words, vendors could gain more customers and increase sales if they rose in Vendor Level, AND they would pay less...
commission fees; it is a profitable prospect which is bound to encourage the vendors to operate honestly.

These levels therefore contributed greatly to encourage honest trade and discourage dishonest sellers, which consequently warrants a successful marketplace (Allodi et al., 2016; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Wehinger, 2011). The higher vendor levels, similar to the levels of trust discussed below, took effort and dedication to attain. The way that the vendor levels were constructed demonstrates how mechanisms, like for example customer feedback, can affect the market structure (see also Allodi et al., 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Radianti, 2010). Because vendors had to have a minimum of 90% positive feedback from customers, they could not scam their way to higher levels; they actually had to ensure customer satisfaction with the product and service they provided in regards to components like price, quality, and time (Beckert & Wehinger, 2013; Holt, 2012; Holt et al., 2016). The feedback mechanism will be further discussed in section 4.6.

The Trust Levels, contrary to the Vendor Levels, were not as transparent in their calculating procedures. According to the administration, the “formula” for how Trust Levels were calculated was not publicised for “obvious reasons”. By stating this, they indicated that they had knowledge about certain possibilities for members to cheat their way to higher trust levels (as suggested by Allodi et al., 2016; Lacson & Jones, 2016; Radianti, 2010). What they did disclose was that the Trust Levels range from 1-10 and work in addition to, and separate from, the Vendor Levels, which means that they were applied to all members; both buyers and sellers. The “general rule”, as they called it, for generating trust related to how active a member was and how many actions a member performed, in addition to voting from other members of the community. The voting for a fellow community member was done by going on their profile and choosing either “Trust” or “Distrust”. Again, the owners limited the capacity to “cheat” by confining the voting only to those of approximately the same level, meaning that someone on Level 1 could vote neither in favour nor against someone on level 5, and vice versa.

Interestingly, the Trust Levels were only introduced as a feature on AlphaBay in November 2015. Prior to this, they operated with something called “Buyer Reputation”, which was a feature only visible to vendors who received an order from a buyer. The buyer reputation system was implemented for the exact purpose of ensuring safe trade for the vendors, since buyers already had an indication of the trustworthiness of a seller through the Vendor Levels. The Trust Levels can therefore be considered as the visualisation of reputation amongst the members of AlphaBay and were thus important for both buyers and sellers (Ablon & Libicki,
Vendors could choose to have their listing visible only for members of, for example, Trust Level 5 and higher, which meant that they could directly exclude anyone belonging to lower levels. Members looking to buy could do the same if they used the search bar on the left hand side, where they could set a Level limit to only include listings of vendors with, for example, Trust Level 5 or higher. According to the owners of AlphaBay these tools were applied for two reasons: 1) to keep Law Enforcement away by making infiltration harder, and 2) to give members the choice to deal with the elite of the market (i.e., those of higher levels). The second purpose here suggests that there might have been a “semi-flat trading structure” instead of a flat trading structure as described by Allodi et al. (2015).

The reason I have chosen to refer to it as a semi-flat trading structure is due to the fact that the market was at its core built as a flat trading structure where all members were able to trade with any member they wished and all listings were available for everyone (Allodi et al., 2015). However, as AlphaBay evolved and became more refined, they also made changes to their trading structure as stated above. At its core, AlphaBay was still flat in the sense that there were no obvious tiers of trading belonging only to certain members based on their perceived skill set, as was the case in the markets Allodi et al. (2015) studied. Yet, I argue that AlphaBay developed into a more semi-flat trading structure where vendors were able to choose at which Trust Level members were allowed to see their listings, and where buyers were allowed to limit their search to only include vendors of certain levels.

The impact these vendor- and trust levels had is important and functioned as an informal mechanism of regulation. They are considered as informal because they are dependent on actors’ activity rather than a governing force (e.g., the administration in online illegal markets or the state in traditional legal markets). They served as the foundation in the decision making processes for buyers and vendors in order to determine whom to initiate trade with; it was an indicator of trustworthiness. In addition, these levels established members’ reputation, which has already been proven to be of vital importance for online illegal market actors (Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2016; Lacson & Jones, 2016; Wehinger, 2011). Reputation is one of the main contributors in establishing trust in both online and offline illegal markets. In the latter reputation is gained through personalised networks (Beckert & Wehinger, 2012; Moeller & Sandberg, 2015; Sandberg, 2012), and in online illegal markets it is often gained and recognised through labels (Allodi et al., 2015; Hardy & Norgaard, 2016; Holt et al., 2016; Wehinger, 2011).

---

20 See screenshot 7 in the appendix
On the forum accompanying the AlphaBay market, members were, as mentioned in section 4.2, labelled according to how much they participated on the forum. This is one way for market actors to recognise reputation (Allodi et al., 2015; Hardy & Norgaard, 2016; Holt et al., 2016; Wehinger, 2011), and in the market itself it could be recognised through the trust- and vendor levels and the customer feedback system. The levels, particularly the vendor levels, were a way of handling the coordination problem of cooperation (Beckert & Wehinger, 2013). This is due to the fact that vendor levels were dependent on both economic aspects (i.e., goods sold and revenue made) and social aspects (i.e., customer feedback, see section 4.6 below). By adding the need for 90% positive feedback rate in order to advance in vendor level, the administration of AlphaBay ensured enforcement of contract and lowered the risks of exchange for its members. Hardy and Norgaard (2016) said that reputation is ‘cheap for honest sellers to obtain, and costly for dishonest sellers to garner’ (2016: 533), which is also true of the trust- and vendor levels on AlphaBay. This need to categorise reputation on a structural level can be considered as part of the general market culture on online illegal markets, and is a fundamental attribute due to the need to establish trust in an inherently anonymous environment.

4.6 Feedback

Although Trust Levels and Vendor Levels were important factors that directly related to members’ reputation, the feedback system is considered to have been an equally important factor (Allodi et al., 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Radianti, 2010). It is also here that the social aspects of the general market culture shines through, as the written feedback functions as short comments of what members of this cybercrime market is actually thinking and expecting from their fellow denizens. As it has already been established, feedback was inherent in the calculation of Vendor Levels, of which vendors were dependent on 90% positive feedback in order to rise to higher levels. Feedback could only be given to a vendor after a sale had been finalised, and one could choose to leave positive, neutral, or negative feedback. Negative feedback directly impacted the reputation of the vendor both because it affected the percentage of positive feedback required in order to rise in levels, and also because other members could see the negative feedback left on a vendor’s profile and thus make a more informed decision on whether or not to initiate trade (Holt, 2012). This means that even though feedback was utilised as part of a mechanism to establish trust, it was also as a mechanism to build trust on its own.
On AlphaBay members could choose to leave comments to all three feedback options, and vendors had the opportunity to reply to the feedback left on their profile. It appeared to be the norm, in fact it seemed to be expected, that if the feedback was of the negative type then one were to leave a description of why one was not pleased with the product and/or vendor. Some vendors commented on this if there was negative feedback left without description (see Figure 10) and used this as an opportunity to argue that the feedback was “invalid” and unnecessary if the buyer didn’t have anything to actually comment.

They often also used the reply feature to downplay negative feedback; defending their reputation by either claiming that the buyer was incompetent or that the customer was, in fact, a rival vendor with a fake account trying to bring him down by affecting his positive feedback score (see Figure 11). This notion of rivals opening fake accounts to either downplay other vendors or build their original profile has been found in other online illegal markets as well (see Holt et al., 2015).

Another important element prevalent in the replies to the negative feedback, also shown in Figure 11, was the vendor highlighting the fact that the customer did not ask for help. Throughout the negative feedback on the vendor accounts analysed for this paper, there were a lot of references to buyers not attempting to contact the seller before leaving negative feedback. Some vendors even claimed that they had attempted to contact the buyer themselves in order to sort out the issue that led to a negative review, without ever getting a reply. These claims can be considered as a way of protecting ones reputation, and consequently ones trustworthiness, as it shows that the vendor tried to sort it out with the buyer. It can also be seen as a false statement made to salvage the reputation.

Positive feedback, as previously established, was important for the level progression of vendors. In addition, it was also an area where customers expressed their gratitude towards the vendor and informed other potential buyers of the positive traits that a particular vendor
possessed. However, differently from negative feedback, it was not expected that the positive feedback was accompanied with a comment. Yet, a lot of customers left a short note with the feedback, and arguably this was where the “true character” of the vendor shone through; it was here they were praised for the services they offered. Interestingly, the praise often included similar constituents as the negative feedback; quality of product, communication with the vendor, price, and customer service or support provided by the vendor. Buyers often displayed signs of loyalty and trustworthiness by claiming that they would trade with a vendor in the future or have traded with them in the past with comments like:

“great vendor great product everything works as described. i will be using this vendor in the future.”

“keep it up bro, will keep coming back”

“Fast shipping. Superb support. Vendor answers private messages in record time. Pleasure to work w/ and would buy from again.”

Vouching for vendors in this manner was a way of acknowledging not only trust but also skill, which is an important attribute of one’s reputation in regards to hacker culture. This will be discussed in greater detail in the next chapter.

Throughout the positive feedback data collected, there were a few feedbacks registered with purely negative comments (see Figure 12). This was found to be especially damaging to a vendor’s reputation because positive feedback could not be removed by the administrators. Even though it counted towards the total percentage of positive feedback needed in order to rise in levels, it still looked bad to the potential buyers looking at a vendor’s listing or profile. On both their listing and user profile it was always the most recent feedback comments that were displayed on their front page.

In addition to appearing in the data, a vendor brought up this issue on the forum, proposing that the administration give vendors the opportunity to make positive feedback ‘private’ if they wished, for the purpose of avoiding situations like the one in Figure 12. These contentions suggest that there were some individuals that took advantage of the feedback system in order to

Figure 12: Positive feedback with negative comments

---

21 A «vouch» is an endorsement from fellow community members and is a term that is often used in this environment.
damage others. If what the member wrote on the forum is true, then this suggests that there are individuals on the market who open accounts just for the purpose of doing harm to others (see Figure 13). This, in turn, affected the functioning of the market and if it was not handled by the regulating force (i.e., the administration), then it could indeed do damage to the market structure and consequently also the success of the market.

4.6.1 Feedback Content

As briefly mentioned above, it was not only the mood of the feedback (i.e., positive, neutral or negative) that was important to the AlphaBay community, but also the content of the feedback left. When analysing the feedback left for vendors dealing in various cybercrime goods and services, I identified five categories that were reoccurring in most, if not all, feedback comments. Four of them were similar to what has been found in previous studies, namely: time, communication, price, and quality (see Beckert & Wehinger, 2012; Holt, 2012). The last concept was not identified in any previous studies on illegal markets, but rather in the literature on hacker culture; skill and commitment. Each of these categories were either highly appreciated or severely criticised by buyers, and they will be discussed in the following sections.

The first category, time, refers to both the speed of which the vendor managed to deliver the goods and services, and to the time buyers had to spend on said good or service. The less time involved the better. Positive feedback often included comments such as: “great fast service, no wait.”, “instant delivery!”, and “did what he said he would and quickly!” These comments were definitely a boost towards vendors’ reputation as quick and reliable sellers. Negative feedback held comments like: “DON’T WASTE YOUR TIME” and “it takes a little while to download”, which of course had a negative impact on the seller’s reputation. I am confident that this focus on the swiftness of a transaction and product (if it is a program for example) can be found on other legal and illegal online markets as well and therefore is part of the general market culture for these markets.
The communication with the vendor, or the availability of the vendor, was also often commented upon in the feedbacks left by customers. This was interestingly enough mostly commented upon in the negative feedback more often than the positive feedback. A lot of the negative feedback entailed comments saying that the vendor never replied to their questions, even after waiting for a (long) while (so also here time is of importance). This resonates with Holt’s (2012) observation of customer service and the concept of support for the customers. He states that the support offered to the customers is an integral part of the overall customer service, which in turn affects the customer feedback (Holt, 2012). Interestingly, vendors on AlphaBay would often reply to these claims by saying that the customer never attempted to contact them (as exemplified in Figure 11) and, that they were probably either “stupid” or “a competing vendor” trying to get their rates down.

The notion of price went hand-in-hand with the (perceived) quality of that product. As discussed earlier, both in terms of economic sociology and previous research, the element of price, or value, is intrinsic within legal and illegal markets alike (Aspers, 2011; Beckert & Wehinger, 2012; Fligstein & Dauter, 2007; Holt, 2012). On AlphaBay, the subject of price was often questioned when an item was considered to be either too cheap or too expensive (see also Holt, 2012). This issue has also been identified by other authors and is considered as an element causing uncertainty not only in relation to the quality of the actual product (Ablon & Libicki, 2015; Holt et al., 2016), but also the trustworthiness of the vendor.

As mentioned previously, the concept of quality was often discussed in relation to the price of the product. One of the coordination problems identified by Beckert & Wehinger (2012) is, as discussed in chapter two, exactly that; assessing product quality and, thus, the value of the product. On AlphaBay, the quality of a product or service often came under scrutiny, especially when it was considered to be bad, or not working at all, but also when it was perceived as good, “exceptional” or “the best on AlphaBay”. The feedback system therefore functioned as a way for market actors to assess product quality through the comments left by other members. Quality, as presented by Holt (2012), is also an intrinsic element in relation to customer service. Therefore, quality is important not only because of the user experience of that particular product or service, but also because of the buyer’s overall impression of the seller. Providing high quality products results in happy customers and, subsequently, increased reputation through higher trust- and vendor levels.

In addition to the elements already established by both Holt (2012) and Beckert & Wehinger (2012), I found another element in the feedback comments that was prevalent and
considered as vital for the vendor's reputation; the skill and commitment of the vendor were intertwined with the other categories listed above. Commitment was often measured by the swiftness of the transaction (i.e., time) and the availability of the vendor after the sale was finalized (i.e., communication). Vendors were often praised for their commitment to the customer, for the skills they had to build, for example, malware, and for the ability of teaching those who were not as tech savvy and perhaps new to the world of cybercrime (this will be discussed in more detail in the next chapter). Sometimes, the commitment of the vendor was praised by the buyer even though the problem couldn’t be solved, because the effort the vendor made to try to solve the problem. Buyers who then had purchased a product they could not use would still compliment the seller for doing all that they could in order to sort out the issues that were causing the difficulties. By being dedicated to customer service in this way, the vendor built a good reputation, which is inherently tied to the trustworthiness of an individual (Ablon & Libicki, 2015; Allodi et al., 2016; Beckert & Wehinger, 2013; Hardy & Norgaard, 2016; Holt, 2012; Radianti, 2010; Wehinger, 2011).

From what has been presented above, it becomes apparent that the feedback system on AlphaBay played a fundamental role to the market structure and to the ways in which market actors made choices regarding purchases and trustworthiness of other actors. Vendors needed to put effort into not only their products, but also their customer service and support in order to warrant positive feedback from buyers. The feedback system clearly works as an informal mechanism to tackle problems of coordination; whether that be assessing quality or reducing the risk of exchange by assessing the reliability, or trustworthiness, of a vendor. I am confident that the first four categories can be found in other online illegal markets, considering their presence in previous research, and be part of a general market culture. In addition, it would be interesting to find out if the final category of skill and commitment might also be part of a general market culture in other markets or if this is indeed unique to the specific market culture of Darknet cybercrime markets alone.
4.7 Concluding remarks

From the information above, it is quite clear that AlphaBay was a well organised and sophisticated market; structured to encourage honest trade and discourage those who were looking to conduct dishonest trade. The administration and owner(s) of the market seemed to be experienced actors on Darknet markets and had thus implemented mechanisms of enforcement and punishment in order to regulate the market, probably improved from other or previous markets (e.g., Silk Road). Anonymity has been identified as simultaneously being the most valuable and most vulnerable element of online illegal markets (Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2016; Holt et al., 2016; Lacson & Jones, 2016; Wehinger, 2011). Due to the issues of trust and problem of cooperation this anonymity brings with it, AlphaBay implemented mechanisms to diminish these issues and thus made the distribution of information less asymmetrical (Akerlof, 1970) and more transparent. Beckert and Wehinger (2012) write that ‘illegal markets are structurally inefficient because of limitations in their potential to develop competitive structures’ because of the information asymmetry and intransparency in terms of validation of quality and value (2012: 17). However, from the findings presented above, I argue that AlphaBay was not subjected to the same information asymmetry and intransparency as illegal markets in the physical world are.

The feedback system provided an arena where customers could express their opinions about goods and services bought, as well as the reliability of the vendor. As my findings demonstrate, customers often commented on the things that has rendered illegal markets structurally inefficient, according to Beckert and Wehinger (2012). They provided honest reviews for potential buyers to evaluate, from which they would gain information on the price and quality of the product or service (i.e., value), the reliability of the vendor (diminishing the risk of exchange), and the skill and commitment of the vendor (for better customer service). Thus, the feedback system functioned as an informal mechanism regulating the marketplace by helping members tackle these problems of coordination.

In addition, the vendor- and trust levels function in the same manner as reputation mechanisms identified in previous research (Allodi, et al., 2015; Hardy & Norgaard, 2016; Radianti, 2010; Wehinger, 2011), and is an essential element in order to establish trust in the market. These formal and informal regulating mechanisms coupled with the mechanisms of punishment are intrinsic elements in order to keep the marketplace manageable for honest sellers and buyers, and cumbersome for rippers and scammers, as has also been found in previous
studies (Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2015; Holt et al., 2016; Radianti, 2010; Wehinger, 2011). These mechanisms are also elements of the general market culture that I expect can be found in other online illegal markets. The rules and mechanisms of enforcement from the administration; the structural feature of trust- and vendor levels to establish reputation and indicate trustworthiness; and the customer feedback system to evaluate the price, quality, reliability and skill of vendor; all have been found in similar capacity on other online illegal markets, and probably will continue to function as ways of tackling coordination problems in future online illegal markets as well.

To conclude, I would argue that the quote at the very beginning of this chapter provides an idea of how much work was put in by the owner(s) and administration in order to perfect an online illegal market. AlphaBay was, on the day it was taken down by law enforcement, the largest and longest lasting Darknet market in history. The structural features and mechanisms of enforcement were clearly efficient in their means, and that is why I believe they will not only be adapted in new, or already existing, marketplaces, but also further developed and refined.
5. The Influence of Hacker Culture

“I vouch for this man. He’s LEGIT. Well written and descriptive guides for each of his methods. Definitely noob friendly.”

(Posted on the forum in support of a vendor)

The following chapter sets out to evaluate the influence hacker culture has on the Darknet market AlphaBay. By looking at the market from a cultural perspective, it is hoped to gain a deeper understanding of the social organisation of the market and how market actors relate to one another. Where the previous chapter focused on the structural features and mechanisms implemented by the owner(s) of AlphaBay in order to tackle coordination problems and how this can be considered as part of general market culture; this chapter looks at the social behaviour of market actors and how the norms and beliefs of market actors shape the marketplace. By looking into the cultural values and norms of the marketplace, elements of a specific market culture was revealed, and arguments for why it is specific to cybercrime markets and not considered as general market culture will be demonstrated throughout. However, there are also some elements of the findings that are applicable to other online illegal markets as well; that are neither unique to cybercrime markets nor part of the general market culture. These instances will be suggested to be specific to online illegal markets as a whole, rather than solely to cybercrime markets. Hacker culture, as presented in chapter two, consists of several communities and collectives of people, with fluid borders making navigating between them easy (Jordan, 2008; Jordan & Taylor, 1998; Holt, 2007; Taylor, 1999; Thomas, 2002; Wall, 2001a; Yar, 2013). This fluidity could also be seen on AlphaBay where members often referred to other hacker forums or markets, either to validate their legitimacy or reputation; or out of genuine curiosity as to who frequented those forums and what kinds of tools and services they distributed.

This chapter has seven subheadings, excluding the concluding remarks, each focusing on categories identified in the data that are subsequently explained by hacker culture and the previous research in the field, and considered as part of a specific market culture.
5.1 Development and Technical Finesse

One of the first categories to emerge out of the data collected for this study, was the vendors’ focus on the development of a product, and the buyers’ focus on, what I call, the technical finesse of a product. Both of these were reoccurring in both the data collected from the feedback system, and the data collected from forum threads. The development and technical finesse mostly referred directly to malicious software and other cybercrime tools. For some market actors it was highly important to continuously work towards a better program, or a better guide, for the purpose of developing the products to be more than they were initially created to be. In regards to malicious software, this was especially important because anti-virus programs often caught up on trends within the malware world and designed their programs to counter the malicious software that were on the market. The focus of vendors, thus, often seemed to be on the development of the product, rather than directly on financial gain.

Figure 124

Figure 14 above is an example collected from a forum thread about a new ransomware being sold on the marketplace. Here, the vendor advised a very enthusiastic buyer not to buy his product, because the work was not finished. Although it is recognised that he still advised the customer to buy the product after it was finished, the fact that he advised against it in the first place is an important point to make. By doing this he showed that the development of a good ransomware was more important than making money off something that was not perfected for optimal usage. This emphasis on development manifested itself through different instances on AlphaBay. The vendor that started the thread where the post above was found, had, similar to many other vendors on the market, offered so-called “voucher copies” before the interaction in Figure 14 took place. Offering such copies was of frequent occurrence on the market and the forum, and this is something I argue is unique to cybercrime markets and thus serve as part of the specific market culture. It was often found that when a new malware or other cybercrime tool was listed on the market, members of AlphaBay would immediately ask for, and expect, voucher copies. These voucher copies would either be given out for free or offered for a cheaper price to a selected amount of members whom volunteered to test the product.
The purpose of this was twofold: on the one hand, it provided extensive reviews that could result in more interested buyers, and on the other hand, and in most cases also more importantly, it provided a possibility for the vendor to get feedback on what needed to be improved. The former (i.e., more interested buyers) can arguably also be found in other markets as well in the form of ‘bulk discount’, free samples, or ‘buy one get one for free’ (Hardy & Norgaard, 2016; Radianti, 2010). In these instances, the vendor advertises, for example, that if you buy \( x \) amount, you get \( y \) for free in order to gain more buyers from lucrative deals in exchange for positive feedback (Hardy & Norgaard, 2016; Radianti, 2010). The latter (i.e., getting feedback on areas of improvement), on the other hand, is unique to cybercrime market. For example, after receiving an extensive review on a ransomware, one vendor replied:

“Great feedback, added on my to-do list”.

This type of back and forth in building, reviewing, altering, and fixing code and tools is an essential element of hacker culture (Jordan, 2008; Taylor, 1999; Thomas, 2002; Yar, 2013), and it is arguably from here that this constant development of products for sale has its origin, or at least its inspiration. It is through this transparency of one’s work that one can gain peer recognition (Jordan, 2008; Jordan & Taylor, 1998), which also was a source of internal reputation on AlphaBay (see section 5.5).

In addition to the above, there is also an element that I, here, refer to as technical finesse, which was greatly appreciated and applauded by members of the community. The technical finesse of a product would not necessarily always be mentioned directly, but often indirectly and in reference to the intellect of its writer. It appeared as short comments in the feedback section of a listing on the marketplace, such as “genius” or “flawless”, and in longer comments on forum threads when customers had bought and tested a product or had received a voucher copy and were obliged to leave a thorough review. For example, in a forum thread discussing a ransomware listed on the market, one member highlighted the genius of the vendor:

“It’s extremely clear how smart this guy is and how much knowledge he has by analyzing his writing skills (which means a lot of reading) and his coding work. Totally genius.”

The vendor’s coding work is linked to the technical finesse of the ransomware, because if it hadn’t been done in a nifty way, then they wouldn’t have been commented on.

This aspect of technical finesse is an element of what has been referred to in the literature as ‘mastery’ (Holt, 2007; Thomas, 2002). It is important to note that it would only be the so-
called ‘high rollers’ or ‘elite’ of the market that would normally comment on the technical finesse of a product, those with less skills in the community were more concerned about how easy or difficult a product was to use or understand. The fact that the member above literally called the coder a genius shows that the way the vendor had built the ransomware was important to members of the forum, at least those who had experience in the field. Interestingly, this ransomware was advertised as being “beginner friendly” and that prior experience was not necessary. Specifically, this is interesting because beginners would find the ransomware working as advertised and be satisfied by that fact, whilst those with experience in coding and programming would probe the software, looking for flaws. When the flaws were not found, or were of minor importance, they applauded the writer and were certain to compliment these writers on their work. This scrutiny and probing of programs and software is intrinsic in hacker culture and the subsequent improvement and development of said artefact is central (Holt, 2007; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002), as discussed above.

These elements of hacker culture clearly influenced the culture of the market; it affected the way in which customers rated products and, in addition, what customers considered important traits in a vendor and his products in order to initiate trade. This relationship between buyers and sellers is central to all market cultures, but it is also unique to specific markets and therefore shapes the specific market cultures of said markets (Aspers, 2011; Sandberg, 2012). Some members would only look for those products that were made for beginners and functioned just as they were described. Other members, who had more experience and knowledge of both the products at hand and most likely other hacking related activities, would look for possibilities of improvement and flaws that needed to be fixed. The latter type of members would never buy a product of someone who was known to have low coding quality, unless it was to deliberately “out” their flawed methods to the community via the forum threads. So not only did the community applaud the focus on development and the technical finesse of a product; they would also tear apart someone’s products, guides or services if they were flawed.

The technical finesse of how something was done showed the level of someone’s skill, and skill is arguably the epitome of knowledge and commitment, which is essential elements in order to create a program or software that will earn admiration (Holt, 2007; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002; Wall, 2001; Yar, 2013). Hence, I believe that in cybercrime markets one will find that technical finesse and development of software will be essential elements in the specific market culture, because it is through these elements that market actors determine the value of a product (see Akerlof, 1970; Aspers, 2011; Beckert & Wehinger,
and the reputation of the vendor (see Allodi et al., 2015; Hardy & Nordgaard, 2016; Holt, 2007; Holt et al., 2016; Jordan, 2008; Radianti, 2010; Thomas, 2002; Wehinger, 2011).

5.2 Knowledge and Information

Gathering and sharing knowledge and information were also two reoccurring and intersecting themes found in the data, mostly from the forum. Here, the emphasis was on market actors’ abilities to accumulate knowledge and information on both the practical issues of AlphaBay market and about certain tools and services being sold on the market. The importance of knowledge and how valuable it was to the members of the market is exemplified in a quote by a rather frustrated member:

“DO YOU GUYS NOT KNOW HOW TO READ BOOKS ON PROGRAMMING AT ALL? While buying something that requires you to program from the get go?”

The quote was gathered from a forum thread about a ransomware for sale and clearly criticises the replies to the thread from those who had bought the software and could not make it work because they did not have the skills to do it. What is interesting about the reply made by the member is that it did not focus on the fact that these people could not code or program, but rather that they seemed uninterested in learning to do so. This is fundamental in hacker culture; they thrive off of curiosity and willingness to expand their knowledge about technological components (Holt, 2007; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002). This willingness to learn, expand ones knowledge, and accumulate information was, as in hacker culture, central amongst members of AlphaBay. Due to the nature of the products that cybercrime markets deal in, I expect this focus on willingness to learn and accumulate knowledge is part of a specific market culture for these markets. I suggest this because it seems to be expected that buyers commit to learning and put in the effort to do so. An additional example came from a member who explained to another member the importance of time and effort:

“I know jackshit about trojans, but I’m willing to take the risk and learn. You need to put in the time to learn how to use it, then you need to put in the time actually using it. The way I see things, the more time and effort you put in, the more you’ll have to gain.”

The forum was used not only by vendors to advertise their products, but also as an environment where members could ask questions and advice of more experienced members.
However, in order to receive sincere answers from more knowledgeable members, you had to demonstrate that you were inclined to learn and to put in the effort needed. This was demonstrated by both of the quotes above, and could be seen, similarly, when someone got scammed by a member that had already been deemed a scammer by the community:

“You deserve to be scammed if you couldn’t READ my posts.”

This quote is collected from a forum thread started by a member claiming to be able to hack emails and social media accounts, to which several pointed out he was a scammer by debunking his flawed methods, as briefly discussed in the previous section. However, despite several warnings, even from reputable members, some still requested his services. In turn, when someone called him out as a scammer because they had been scammed after having bought his services, one of the reputable members clearly stated that they deserved to be scammed because they had not bothered to gather the information about the vendor that was readily available to them on the forum thread. Not looking for the information needed to make an educated decision about a vendor, or about a product sold, was frowned upon and was considered as a lack of commitment to accumulate the proper information (see also Holt, 2007: 186). As mentioned previously, commitment is measured in both the time and effort someone invests into something, whether it be finding information or using a malware.

Consequently, by not looking for the information needed, especially when it is readily available as in the example above, one is deemed deserving of whatever misfortune ones lack of commitment causes. In hacker culture, asking questions and finding information on forums is an indication of commitment according to Holt (2007: 186), and it is precisely this notion that was criticised on AlphaBay when members were not committed enough to look for information. Arguably, this aspect of the hacker culture influenced the market culture in the way that it not only considered looking for information and expanding ones knowledge as essential, but rather as expected. And it is this expectation of market behaviour that makes this an element of a specific market culture (Aspers, 2011).
5.3 **Skill**

The concept of skill emerged in all kinds of situations both on the marketplace and on the forum. It bears resonance to the notion of technical finesse discussed in section 5.1, but also differs from it because here it refers more directly to the perceived skill level of a market actor, rather than the recognised skill of a vendor based on his coding abilities. A members’ skill level was something that was almost constantly under scrutiny, both positively as in section 5.1 for example, and negatively as will be seen in section 5.6. When a member’s skill level was not directly mentioned, it would often be demonstrated through the use of names and labels, of which noob, newbie, and script kiddie were the most frequent. These labels originally have a negative connotation to them (Furnell, 2010; Holt, 2007; Jordan, 2008; Taylor, 1999; Thomas, 2002; Yar, 2013), but it all depended on the context in which they were used. For example, listings would often advertise as being “noob friendly”, meaning that the product or service was made just as much for those with little to no experience with hacking. In fact, most of the listings collected for this study contained reassurances that the product could be used, or a skill could be learned, by those who did not have previous experience in the field (see Figure 15). This is interesting because, in hacker culture, skills are the basis of judging your knowledge not only of technology, but also of hacking tools, techniques, and language (Holt, 2007; Thomas, 2002).

![Figure 15: No previous knowledge needed for operating this ransomware](image_url)

Script-kiddies are often considered to be low level hackers whom do not have the skill set to actually code or perform hacks (Furnell, 2003; Jordan, 2008; Thomas, 2002). Yet, the vendor in Figure 15 reassures him that he is indeed knowledgeable enough to buy this ransomware because he built it for those who have even less experience with malware. Indeed, this was very often the case on malware listings in the market, where they would advertise their cybercrime tools as being “noob friendly” and possible for “anyone” to use. This is interesting particularly when seen in opposition to the importance members still placed on the technical finesse of a product. It causes a paradox of skill sets needed and expected. Skill, in hacker culture, is considered as the epitome of knowledge and commitment, a display of mastery, and as a profound understanding for technological elegance and development (Holt, 2007; Jordan, 2008;
Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002). But for the users of certain products, skill is no longer important; the tools are made so that anyone can use them (see also Ablon & Libicki, 2015; Allodi et al., 2015). In this way, then, one could argue that the specific market culture of cybercrime markets expected skilled coders and technically elegant products. Whilst the costumers of cybercrime markets were not expected to have any previous experience or skills, and thus represented part of a general market culture through which they would receive customer support and help as in any other online market (see Bakken, 2015; Hardy & Norgaard, 2016; Lacson & Jones, 2016). Vendors could indeed be called out for being fake, or scammers, if they did not possess the skills necessary to help customers with the products they had bought from them.

This lack of ability to prove one’s skill by teaching others has also been found in hacker culture as something that would have a negative impact on the person in question (Jordan, 2008: 30). On AlphaBay, it would result in negative feedback on the market listing and also séances of flaming from more reputable members on the forum threads, which would affect his internal reputation severely. Thus, technological knowledge and the accompanying skill set, as identified in hacker culture, expected of vendors selling cybercrime tools and services influenced market actors to judge other members according to these cultural values.

5.4 Outsiders

The notion of ‘outsiders’ emerged on the forum threads, where market actors would judge each other according to how one behaved and responded to other members. If someone behaved differently than expected or had a different way of phrasing themselves, they would often be subjected to accusations of not belonging in the community, or more specifically on the marketplace. Often, members were accused of being law enforcement looking for information, or ‘snitches’ providing information for law enforcement. In other instances, someone would be told directly or indirectly that they did not belong in this environment for various reasons. For example, in a heated discussion on a forum thread regarding a hacking service, several members were arguing against one member who requested the hacking service and someone eventually wrote:

“No, I’m telling you to fuck off and die. You are too dumb for darkweb”.

These kinds of insults were frequent when someone did, said, or claimed something that others in the community collectively disagreed on or regarded as obviously wrong (see also section 5.6).
In these cases, then, the response of the other market actors would be in a manner that expressed their sincere dislike for not only the comments or claims made, but also a total disregard to that member’s belonging in the community; they were considered as outsiders rather than insiders of the community. In a highly secretive environment where anonymity is both a strength and vulnerability, these means of identifying who is part of the community and not, are essential (Holt, 2007; Taylor, 1999). Indeed, it is quite common in hacker communities to test other people’s knowledge both in regards to technology and in regards to the norms and values of hacker culture (Jordan, 2008; Thomas, 2002). Those who cannot pass these tests are deemed ‘fake’ and not considered as part of the community.

In addition to knowledge and norms, language was also an important element for market actors in their analysis of others. For instance, when someone wrote in a very formal manner, they were viewed with scepticism and other members would comment upon the formality and even mock it because it was out of place. A good example of this was when a member left a post in a forum thread asking the starter of the thread a few questions, which was normal, but he ended the post writing “waiting for your reply” followed by his handle (i.e., username). This formal way of ending a post was immediately commented upon, and it raised suspicion amongst other market actors. One of the members wrote in a mocking tone:

“Waiting for your reply!? Who the fuck writes that!!”

Implied in this comment was the fact that this was not the way people of this community communicated with each other, it suggests that this person was an outsider; someone who was not accustomed to the culturally appropriate argot. Bad English spelling or grammar, on the other hand, was something that mostly went unrecognised, and didn’t seem out of the ordinary. Language is seen as an important attribute to determine someone’s place in hacker culture, whether it is incorporating leet-speak, hacker jargon, or just a general way of expressing oneself that is considered appropriate to the culture (Jordan, 2008; Thomas, 2002). These expectations of how to phrase oneself, I suggest, is unique to different markets and therefore the above influences the specific market culture of cybercrime markets. It is clearly intertwined with the other elements already discussed (i.e., knowledge and skill), and thus further underlines my arguments that elements of hacker culture influences the market culture of cybercrime markets.

Further, the possible presence of law enforcement was another issue that caused market actors to accuse someone of being outsiders (i.e., working for law enforcement agencies). Requests for a meet-up in the physical world were particularly frowned upon and almost
immediately linked to law enforcement. In one particular discussion on a forum thread about a ransomware there was a relatively heated discussion between a potential buyer, the vendor, and a few other members who had joined in to defend the vendor. Here, the customer asked to meet the vendor in the physical world so that the vendor could show him how the ransomware worked. The vendor, of course, declined the request proposing online tutoring instead, and other members of the forum were quick to accuse the customer of being an affiliate of law enforcement trying to pin down the writer of this especially damaging ransomware. The customer retaliated and bragged about being a “real criminal” that had done time in jail and that they were only “scaredy-cats” hiding behind their keyboards and screens. The discussion went on for quite a while and engaged several members of the market. In one comment a member replying to the bragging customer highlighted several important elements of secrecy (see Holt, 2007; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002):

“If I’m being honest, the more you write the more you strike me as LE. You’re putting too much effort to try to meet [the vendor] personally while trying to strike his nerve. Are you hoping to have him engage you in an argument so he carelessly reveals himself [?] And why are you so comfortable releasing so much personal info in public like this, proves you have little or no worries for LE[.] Be honest, did you strike a deal to get out of jail early while helping them track down infamous coders, are they helping you type out these long sentences on a sales thread of a product you’ve never used before[?] […] PSA to all other users, be careful with this one. he may not be LE but he’s too loud and careless, you may not want to be exchanging certain info with him.”

It becomes clear through the criticism that this member had acted in a manner that made him stand out suspiciously. As mentioned above, the effort put in to meet someone in the physical world functions as a clear indicator for other members of the market that someone might be law enforcement. Also, the issue of secrecy for personal reasons is highlighted; staying anonymous and limiting the sharing of personal information was not only emphasised by the administration of AlphaBay, but it is also a value which is intrinsic in hacker culture because of the illegality of the activities they often are involved with (Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002; Wall 2001a; Yar, 2013). The member accused of being law enforcement was considered to be too eager to give up personal information, which in turn could mean that he had little regards to law enforcement and might, in fact, operate as an informant for law enforcement agencies. Lastly, a warning was ushered to other users not to get involved with this member because of his disregard for the value of secrecy as a safety precaution (see Holt, 2007; Taylor,
These elements of concern for market actors often pointed towards law enforcement, and accusing someone of being law enforcement happened quite frequently on the forum.

From the discussion above, it is clear that the elements of secrecy and law enforcement identified in the literature on hacker culture had an influential role on AlphaBay. It affected the way in which market actors assessed the trustworthiness of other market actors, which was an important element of the market structure identified in the previous chapter. A paradox is created when the anonymity that is so important for the element of secrecy also is one of reasons for a highly sceptical environment (Holt, 2007; Jordan, 2008; Taylor, 1999; Thomas, 2002). Anonymity and secrecy were some of the reasons that the AlphaBay market operated as smoothly as it did, as has also been identified in the previous research on illegal markets operating online (Ablon & Libicki, 2015; Allodi et al., 2015). At the same time, the scepticism and scrutiny of someone’s behaviour has become members’ security. Thomas (2002) explains this paradox of secrecy and trust in an elegant manner: ‘In a kind of Orwellian doublespeak, secrecy has become freedom, and the need for security (through implicit distrust of others) has become trust’ (2002: 34).

It is important to note, here, that the issue of law enforcement is something that is likely present in all online illegal markets. Although these issues are highly important in hacker culture, I cannot argue that it is part of a specific market culture for cybercrime markets. Rather, I suggest that it is part of a specific market culture for all online illegal markets. Illegal actions demand consideration of legal retribution, and therefore it would be academically ignorant to argue otherwise. Hence, I argue that issues of law enforcement and mechanisms such as anonymity are part of a broader specific market culture for online illegal markets. But, I also propose that the way in which market actors identify possible law enforcement officers, or other outsiders, is unique to different markets and that hacker cultural norms and beliefs influence these processes in cybercrime markets.

5.5 Reputation

In the data collected for this study, I found two types of reputation: internal and external. Internal reputation refers to the type of reputation members built inside the community, including that which was transferred from other Darknet markets (see also Ablon & Libicki, 2015; Radianti, 2010). External reputation, as implied by the phrase, refers to the attention a vendor or a malware received outside of the Darknet; in the mainstream media and on the
Clearnet. Reputation, both internal and external, was not necessarily directly aimed at the username of a vendor, but often towards a specific malware or other cybercrime service.

Internal reputation could be built partially through the structural features of the market, as discussed in the previous chapter, but also to a large extent through involvement on the forum, where one’s true knowledge and skill level could be scrutinised in order to either be debunked or confirmed. The latter of which was particularly important for those members who were relatively new to AlphaBay and had not been able to escalate their vendor level and trust level (see Figure 16).

In the example above, the user who claimed to be able to hack email addresses was criticised due to his lack of internal reputation. He was not known from any other cybercrime markets or forums, and he could not provide any proof of his skills, as is demanded in order to gain recognition in hacker culture (see Thomas, 2002: 91). Internal reputation can be considered as the AlphaBay equivalent of peer recognition often emphasised in the literature on hacker culture (Jordan, 2008; Jordan & Taylor, 1998; Thomas, 2002; Wall, 2001; Yar, 2013). As briefly mentioned above, internal reputation could be transferred from other Darknet markets or forums (see also Radianti, 2010: 194), and in such cases members whom knew a new member from another forum or market would be quick to support a member’s claim of reputation, or rather knowledge and skill level.

In addition, getting “vouches” from higher ranking members by getting products or services reviewed, as discussed previously in section 5.1 above, also would boost someone’s internal reputation if the product was considered to be of good quality (see also the quote at the beginning of this chapter). The higher status of the member vouching for another member, the higher the influence would be on the internal reputation. For example, in Figure 17 below, a member listed all the reasons to buy a botnet advertised by a new member of AlphaBay (but renowned in other markets), where point number 2 maintains that the administration had vouched for this vendor, which was the highest possible vouch one could receive. Along with this internal reputation boost, the elimination of one of the risks of exchange (i.e., payment method, discussed in the previous chapter), and external reputation, there were, according to this member, no reasons not to buy this botnet. This example demonstrates the influence of peer

---

**Figure 16: Member criticising someone who has not built his reputation**

You registered yesterday and suddenly you can hack email addresses???? LOL you must be a genius 😑

---

In the example above, the user who claimed to be able to hack email addresses was criticised due to his lack of internal reputation. He was not known from any other cybercrime markets or forums, and he could not provide any proof of his skills, as is demanded in order to gain recognition in hacker culture (see Thomas, 2002: 91). Internal reputation can be considered as the AlphaBay equivalent of peer recognition often emphasised in the literature on hacker culture (Jordan, 2008; Jordan & Taylor, 1998; Thomas, 2002; Wall, 2001; Yar, 2013). As briefly mentioned above, internal reputation could be transferred from other Darknet markets or forums (see also Radianti, 2010: 194), and in such cases members whom knew a new member from another forum or market would be quick to support a member’s claim of reputation, or rather knowledge and skill level.

In addition, getting “vouches” from higher ranking members by getting products or services reviewed, as discussed previously in section 5.1 above, also would boost someone’s internal reputation if the product was considered to be of good quality (see also the quote at the beginning of this chapter). The higher status of the member vouching for another member, the higher the influence would be on the internal reputation. For example, in Figure 17 below, a member listed all the reasons to buy a botnet advertised by a new member of AlphaBay (but renowned in other markets), where point number 2 maintains that the administration had vouched for this vendor, which was the highest possible vouch one could receive. Along with this internal reputation boost, the elimination of one of the risks of exchange (i.e., payment method, discussed in the previous chapter), and external reputation, there were, according to this member, no reasons not to buy this botnet. This example demonstrates the influence of peer
recognition on the market. Albeit reputation has been proven to be an exceedingly important attribute in online illegal markets as a regulating mechanism (Allodi et al., 2015; Hardy & Norgaard, 2016; Wehinger, 2011), the internal reputation presented here has a different function. Here, internal reputation works as a means of proving the skills of the vendor selling this botnet, and that is what is important in hacker culture: to be recognised for your skill and knowledge (Holt, 2007; Jordan, 2008; Thomas, 2002; Wall, 2001a; Yar, 2013).

![said:](image)

| Can you give me an idea of what the webinject and ATS code looks like? |

You honestly don't need any of that, the bot is working perfectly, he is a very old and good coder and besides that:

1. Full escrow if offered.
2. All the head admins are vouching from him
3. The world-wide-news are talking about this bot and the damages that it is making

Any other reasons needed?

Just buy it and stfu.

Figure 17: Reasons to buy bot

The third point listed in Figure 17 used the external reputation of the botnet as a reason for why someone should buy the product; thus the worldwide media functions as proof of malware and other cybercrime services’ success. This was of frequent occurrence on the forum; vendors would post links to news articles about their products and applaud the buyers for their spreading skills. External reputation functioned not only as proof of the product’s legitimacy, but also as a means to boost the internal reputation; by showing the damage a product causes, the vendor had unprecedented proof of its efficiency and quality, which in turn enhanced the vendor’s internal reputation.

Indeed, other members would frequently post in a forum thread if they had noticed a certain product in the news. One member found the damage caused by a ransomware particularly entertaining as he wrote: “HAHAHA!! THE FUCKING CARNAGE THIS HAS CAUSED!!!!” with following links to news articles about the ransomware. Fellow market actors would often reply to posts about products making the news in a positive manner, praising the vendor for the brilliant cybercrime tool. This attention from the mainstream media towards a certain product and the subsequent reputation boost earned by the vendor of said product, can be seen as a parallel to the reputation boost hackers gain from being ‘wanted’ by law enforcement agencies.
In these cases, hackers who had done something so big and incriminating that they were seen as a threat by the police, gained massive amounts of respect and peer recognition within the hacker community (Jordan, 2008; Jordan & Taylor, 1998; Thomas, 2002). On AlphaBay, the attention from outside media had a similar effect as it functioned as proof of someone’s coding skills and their deserving of respect.

However, the external reputation also caused a rift in the AlphaBay community; even though many members praised the vendors for getting their products “famous”, other members ushered words of caution. Getting one’s work published in the media was a breach of the value of secrecy. These contradicting opinions on external reputation has also been found in hacker culture, where some argue that if you are known to the police or other law enforcement agencies, then you are not a good hacker (Holt, 2007; Taylor, 1999). Caution was therefore often mentioned in relation to law enforcement, with reference to the amount of information that was often found in the news articles would suggest that law enforcement could be watching AlphaBay, and thus members should be vigilant. Others directly criticised vendors for not being more subtle about their products, for example criticising the fact that they wrote the official name of the ransomware in the text that showed up on the victim’s computer. Their arguments were often followed with the issues of victims then being able to search the name of the ransomware on the Clearnet, and subsequently, because it had gotten famous, find a way of getting rid of it and save their files without paying the one who was behind the ransomware. As one member put it:

“*There is nothing good of being famous in Clearnet bro*”

These kinds of reproaches focused on the technological tool itself, rather than on the consequences this fame could have on the vendor or the customers using a product. The critique was expressed because the attention from media outlets and on the Clearnet in general would result in the product having a shorter lifespan. Because it would discovered more quickly and thus information on how to limit the damage or avoid having to pay the perpetrator would be readily available to the victims. One aspect the critiques on external reputation did have in common, though, was that they underlined the issue of *secrecy* (Holt, 2007; Jordan, 2008; Taylor, 1999). Whether the presence of law enforcement was the issue or information about how the victim could save his files were the main argument, they both revolved around secrecy. This, again, demonstrates the value of secrecy, and even the possibility that this kind of attention could disrupt the market because of law enforcement interference.
Internal and external reputation, then, shaped the market with the notion that it influenced the way in which the market actors related to one another. Internal reputation in a way equals trustworthiness, which was discussed in the previous chapter and in the literature as one of the most vital elements of illegal markets (Allodi et al., 2015; Bakken, 2015; Beckert & Wehinger, 2012; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Moeller & Sandberg, 2015; Radianti, 2010; Sandberg, 2012; Wehinger, 2011). It directly influenced market actors’ decision making when determining who to trust, in relation to information gathering and possible market transactions. The members with good internal reputation were knowledgeable and skilled individuals from whom one could take sound advice and gather relevant information from, both about the technicalities of the trade and about other members. External reputation, on the other hand, has a more complex impact on the members of AlphaBay as it was either seen as the best way of legitimising the efficiency and value of a product, or seen as a threat to the secrecy of the Darknet market and disruptive of the cybercrime activities that AlphaBay traded in.

Hence, reputation as conceptualised above fits both into the general market culture and the specific market culture, with some minor details setting them apart. The reference to, and building of, internal reputation is part of the general market culture because it was inherent in the structural features of AlphaBay as a mechanism to signal trust, as discussed in the previous chapter. In addition, getting acknowledgement from higher ranking members of a market has been found to boost reputation on other online illegal markets as well (Holt, 2012; Holt et al., 2016; Radianti, 2010). However, I will suggest that the focus on external reputation, and the effect external reputation had on the internal reputation, is unique to the specific market culture for cybercrime markets. This need to brag and get recognition from peers by showing proof of discovery, in a sense, is typical in hacker culture (Jordan, 2008; Thomas, 2002) and has thus influenced the market culture of cybercrime markets.

5.6 Flaming

The notion of ‘flaming’ was found throughout the data, on both the forum and the market, in various forms; some were obvious and others, like in the example below, were a little more discreet but nonetheless efficient in their purpose. It is an element that is present in almost all of the previous sections, and is of importance to the next and final section of this chapter as well. Flaming was a way of expressing oneself towards another member of the market in an insulting but preferably clever manner, often attacking the recipient for stupidity and lack of skill.
It also, paradoxically, sometimes attacked the receiver for being too “feminine”, at the same time as they were also assumed to be male. Flaming has been suggested in the literature to be a vice caused by anonymity and secrecy (Taylor, 1999: 31), by which it is meant that it is easier to start criticising someone and throwing around insults when you are anonymous and you don’t know the person you’re attacking, also referred to as ‘deindividuation’ (Lacson & Jones, 2016: 47).

Flaming could be found in a less direct hostile form, where sarcasm was the “weapon of choice”. For example, when some members were criticising a vendor offering hacking services for a too high price, another member commented:

“This really made me laugh. You idiots do realize you’re hiring a team of hackers to perform something illegal on your behalf right?! LOL. They can charge how they please! Good arguments. Really. Excellent. Unfortunately, fools like this are what makes hacking crews frustrated because the clientele is literally, retarded.”

As opposed to harsher flaming using a row of insulting phrases and curse words, this type of flaming was used to dumb down the arguments of other members rather than attempting to “out shout” them. These ‘flames’ were not typically intimidating or threatening, but rather statements exemplifying the lower IQ of the opposing side.

Figure 18, on the other hand, shows a more classic example of flaming, where a member lashed out with all kinds of insults at his counterpart. This extract is taken quite far into a discussion between to individuals on a forum thread, before eventually being interrupted by another member who criticised one of the participants for going too far on the flaming by calling him a “keyboard warrior”. A keyboard warrior is someone who is particularly aggressive when “hiding” behind a computer screen and his keyboard, and often considered to be cowardly in real life (i.e. in the physical world). This expression is, arguably, the personification of Taylor’s (1999) argument that flaming is caused by anonymity, and made its appearance whenever someone seemed to try too hard to insult someone else, like in the example below.

![Figure 18: Flaming](image)

It seemed, therefore, on several occasions that the line between flaming and keyboard warrior was quite fine and that some members had difficulties navigating this boundary. Flaming is a way of expressing oneself and, as it turns out, there are certain expectations to this element as well.
What is of particular interest, here, is that the member trying to flame has clearly stepped outside the invisible bounds for what is considered appropriate for flaming. Considering other members often pointed out when someone went too far indicates that there was some sort of consensus as to what constituted good flaming and bad flaming. Clearly, from the example in Figure 18, flaming was not just about spitting out as many threatening and insulting phrases as one could, but also about knowing when and how to flame in order for it to be accepted. Flaming could also be used in order to establish authority in regards to masculinity, which will be discussed in more detail in section 5.7 below.

Due to the importance of the *when* and the *how* of flaming, I would argue that it is part of the broader specific market culture of online illegal markets (Aspers, 2011). As it has been pointed out in the literature, although flaming is an intrinsic element in hacker culture, it is also used in other online communities (Jordan, 2008: 125). Therefore, I expect instances of flaming will be present in other online illegal markets as well, but perhaps the content of the insults would be different? It certainly would be interesting to explore.

### 5.7 Masculinity

The notion of masculinity was constantly present on both the marketplace and the forum. It most frequently took place in underlying masculine tendencies that were challenging to pin down and explain at first, because it was difficult to see exactly the reasons for why the environment felt like it perpetuated hegemonic masculinity (Connell, 1987). However, the evidence made it to the surface not only through my own experience, but also through the market actors’ behaviour and language. For example, on the user profiles, members could choose to add their ‘gender’, but most chose not to and the few that had listed it were listed as ‘male’. In addition, not once did I find reference to female members, neither on the forum nor on the marketplace. Although gender in general was not listed or mentioned on people’s profiles, it was natural to assume that the members were male, which was exemplified by the constant reference to the male pronoun and the usage of terms like ‘bro’ and ‘mate’. Only in séances of flaming did expressions referring to females occur; in these instances words like ‘bitch’, ‘pussy’, and ‘cunt’ were used repeatedly. In addition, there were also a lot of references to male dominance, specifically by referencing to the male genitals; phrases like “suck my dick” were of particular high occurrence.
The literature suggests that by using these gendered words, members establish their male authority (Cere, 2003; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Taylor, 2003; Thomas, 2002; Yar, 2013). An example of the use of gendered language when flaming someone is given in the quote below where a vendor replies to a negative feedback on his listing:

“Whiny cunt stalked me every step of the process. He spent more time SE’ing my nuts in his mouth, faggot.”

Apart from the obvious strong language, there are some analytically interesting points about these kinds of replies. First, it starts off using a misogynistic phrase to exemplify the impression of how the customer is (i.e., a “whiny cunt”). Second, it demonstrates the maleness of the composer by referring to his own genitals, before using ‘faggot’ as a shaming mechanism to propagate hegemonic masculinity (Connell, 1987). This type of flaming was very common on AlphaBay, and I suspect one would find it in other Darknet markets as well, due to the fact that anonymity reduces the threshold for insults and that flaming has already been established as an element of expression in other online communities (Taylor, 1999; Lacson & Jones, 2016). Thus, misogynistic language, I would argue, is unfortunately part of the broader specific market culture of online illegal markets, and possibly also legal markets operating online.

The subject of masculinity was also present in practically all the books and articles read on the subject of hacker culture and the computer underground. It is apparent that the atmosphere in the computer underground is highly misogynistic, the area of expertise is male dominated with very few women participating, and the culture thus reflects these imbalances (Cere, 2003; Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Taylor, 2003; Thomas, 2002; Yar, 2013). Although I have already suggested that misogynistic language is part of the broader specific market culture of Darknet markets, I will also argue that hegemonic masculinity is unique to the specific market culture of cybercrime markets. From the discussions provided throughout this chapter, it becomes increasingly apparent that the traits of knowledge, skill, and mastery, as displayed on AlphaBay, are all qualities of hegemonic masculinity similar to that identified in hacker culture (Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999, Thomas, 2002). That is not to say that females are not welcome in this environment, but rather that they must adopt masculine behaviour in order to be successful in their cybercriminal activities. Social Engineering, for example, is suggested to explicitly require a male authoritative voice in order to be successful (Thomas, 2002: 63-64). It is not my intention to suggest that other markets are not as male dominated as cybercrime markets, however studies have demonstrated a more open presence of female dealers in other markets (see e.g., Sandberg, 2012). It would be interesting, therefore, to
see a more in-depth analysis of gender in Darknet markets in order to confirm or refute my arguments.

Due to the anonymous nature of AlphaBay, and other Darknet markets, it is impossible to know how many female members there are, but I am confident that they are present. But, as mentioned previously, they are most likely conforming to the masculine environment in order not to stand out. It could also be the case that they are present, and possibly even respected to a great extent, but by chance have not made an appearance on the data for this study. Nevertheless, as mentioned above, hacker culture is dominated by masculinity and misogyny, and this seems to leave a footprint in the specific market culture for Darknet cybercrime markets; it perpetuates gendered language both in pronouns and comradery, as well as in flaming, and drives the assumption that fellow market actors are male.

5.8 Concluding Remarks

The comment made by a member of AlphaBay displayed at the beginning of this chapter, is in many ways an example of several of the issues discussed above. In one comment, the member managed to show both elements of hacker culture that influenced the marketplace, and elements of the market culture that is not generally part of hacker culture. In other words, hacker culture influenced the market culture to a certain extent, but not exceptionally. There were many elements of hacker culture that were found on AlphaBay that are likely present on other online illegal markets as well; most notably those of flaming, law enforcement and internal reputation. These are all considered as part of a broader specific market culture for online illegal markets. Reputation has already been established as an absolutely vital element of online illegal markets, both in the previous chapter of this thesis and in the existing literature (Ablon & Libicki, 2015; Allodi et al., 2015; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Lacson & Jones, 2016; Radianti, 2010; Wehinger, 2011). External reputation, on the other hand, I have failed to identify in the existing literature, apart from that of hacker culture where attention from law enforcement is considered as proof of ones skills (Thomas, 2002: 91), and is therefore considered as an element of the specific market culture for cybercrime markets.

The most prominent features of specific market culture identified above is the focus on the development and technical finesse of a product, the importance of skill and how the perception of skill influences market actors’ opinion of one another. These aspects are deeply
rooted in hacker culture, and they dictate how market actors relate to each other, as well as influence the reputation of a member. Similar to how actors on legal markets have expectations of ‘who pays for lunch’ or ‘how people talk’ (Aspers, 2011: 94), so too do market actors on cybercrime markets expect certain norms and behaviour. Of most prominence is the feature of ‘voucher copies’, which were expected to be given or sold cheap by all vendors so that its value and quality could be assessed by market actors already proven to be skilled and knowledgeable. In addition, one was expected to phrase oneself in a certain way in order to be considered as an insider rather than an outsider of the community. In other words, one had to prove ones mastery of the social environment as well as the technological tools (Holt, 2007; Thomas, 2002). In addition, members, vendors especially, had to display commitment, skill, mastery, and knowledge in order to be considered as trustworthy and to build their reputation. This was also applicable for those who claimed to be knowledgeable on the forum, whether they were vendors or buyers; they would be deemed as ‘noob’ or ‘fake’ if they could not prove their claim of skill or knowledge.

To conclude, although some elements of hacker culture clearly resonates with a broader specific market culture for online illegal markets, there are also some quite unique elements that would not necessarily be found on other markets. Values such as technology, skill, mastery, knowledge and secrecy, adopted from hacker culture, I argue, have indeed influenced the Darknet markets for cybercrime tools and services.
6. Discussion and Conclusion

This final chapter sets out to summarise, discuss and conclude the findings presented in the previous chapters, and, consequently, provide a clear resolution to the aim and objectives set for the thesis. Using the notion of general market culture and specific market culture has served as a fruitful backdrop for the analysis and the distinction between the two on cybercrime and other online illegal markets will be further deliberated below. The first part of this chapter will therefore thoroughly go through the elements of general and specific market culture identified in the previous chapters, before lifting the perspective of the thesis from the narrow approach I have used throughout, to seeing the findings in a broader criminological context. The chapter finishes with summarising and concluding the paper.

6.1 General Market Culture

As already established, when analysing the structural features and mechanisms of enforcement on AlphaBay, it was hoped to recognise a general market culture based on how the market tackles the coordination problems faced by market actors. By comparing my findings to that found in previous research, I was able to investigate and identify the formal and informal mechanisms implemented to regulate the marketplace. The most prominent mechanisms were: staff regulation in form of rules and punishment, payment method, feedback system, and vendor- and trust levels. In addition, the constant underlying element of reputation was also evident in the regulation of the market as a self-regulating mechanism (see Wehinger, 2011). Reputation was estimated both through formal mechanisms such as feedback, trust levels, and member labels on the forum, and through informal mechanisms influenced by hacker culture (e.g., vouches or proof of skill). Because of the inherent anonymous nature of online illegal markets, reputation serves as a way for market actors to evaluate the trustworthiness of other market actors, which is at the core of illegal markets both online and offline (Allodi et al., 2015; Bakken, 2015; Beckert & Wehinger, 2011; Hardy & Norgaard, 2016; Holt, 2012; Holt, et al., 2016; Moeller & Sandberg, 2015; Radianti, 2010; Sandberg, 2012; Wehinger, 2011). The structural features of AlphaBay and
other online illegal markets, in turn, serve as a source for market actors to build their reputation as well as evaluate other members’ reputation.

One of the greatest weaknesses of traditional illegal markets is what Akerlof (1970) called ‘information asymmetry’ and what Beckert and Wehinger (2012) have referred to as ‘intransparency’ regarding price and quality validation. This, they argue, is what renders illegal markets structurally inefficient (2012: 17). However, I argue that online illegal markets, on the other hand, have developed structural features and mechanisms of enforcement that battle the coordination problems that render these markets inefficient, and have thus established a more stable marketplace where product validation is more transparent. This transparency of product validation has also been identified on the Darknet drug market Silk Road (see Aldrige et al., 2017). Through trust- and vendor levels, and the possibility of adding a written comment to the customer feedback, the structural features of the market ensures transparency. Of course, market actors must still evaluate the accuracy of the information provided for them, but because of the importance of reputation in order to be successful on the market these mechanisms encourage honest behaviour and thus a more efficient market. Therefore, AlphaBay and other online illegal markets are more transparent than their offline equivalents; which provides a better environment for competition (Beckert & Wehinger, 2011). Competition, as we know, is a vital element for all markets.

6.2 Specific Market Culture

The specific market culture of cybercrime markets was expected to be found through the application of hacker culture on the data collected. But rather than just identifying the specific market culture of cybercrime markets, I also found elements that are specific to illegal markets as a whole and to other illegal markets operating online. In other words, the specificity of the market culture is layered like an upside-down pyramid (see figure 19). At the top are the elements that are present in most illegal markets, such as the issue of law enforcement. In the middle are the elements that are specific to online illegal markets in general, that this thesis suggests will be found in other online illegal market as well as cybercrime markets; for example flaming. At the bottom of the triangle is that which is unique to cybercrime markets. Here, elements such as expectancy of voucher copies, commitment to technological development, and willingness to learn, are central. The bottom of the pyramid will change according to which market you study, if
the study is about online drug markets; it would be the specific market culture of drug markets in the bottom.

The simultaneously feared and expected presence of law enforcement is an element that I found in the analysis of the forum threads, as discussed in chapter five, that quickly emerged as part of a broader specific market culture rather than a unique element of cybercrime markets. Although it is considered as an intrinsic element of hacker culture, it is also an issue present in other illegal markets plainly because of their illegal nature. All illegal markets are dependent on trust, not only because of the risk of being scammed, but also because of the threat of being caught by law enforcement. Thus, all illegal markets are forced to consider the possibility of law enforcement infiltration, and be able to identify these possible intrusions or disruptions. This, I argue is dependent on the specific culture of the market. In Sandberg’s (2012) study on culture in the illegal drug trade, for example, market actors are dependent upon the specific market culture in order to identify potential buyers and sellers. I would suspect that they use the same cultural understanding to also identify members on law enforcement. Thus, as discussed in chapter five, I argue that the issue of law enforcement is part of a broader specific market culture of illegal markets, but the means of identifying possible members of law enforcement is dependent upon the unique market culture.

Interestingly, when analysing the communication between members on the forum, I found that their behaviour perpetuated not only elements of hacker culture but an element that is most likely a vice of all anonymous online environments; flaming. As discussed in chapter five, flaming is part of a broader specific market culture of online illegal markets. Although some of the content of the insults found in the data for this thesis are unique to cybercrime markets (e.g., level of technological knowledge and skill), the propagation of misogynistic language in the data is also expected to be present in other online illegal markets. In fact, flaming has already been identified on the former online drug market Silk Road by Lacson and Jones (2016), as well as in ‘other online communities’ by Jordan (2008: 125). Thus, I believe it is safe to argue that this
element of the market culture of AlphaBay will also be found in both existing online illegal markets and in future online illegal markets.

In regards to the bottom of the pyramid, and that which I initially set out to identify, the specific market culture of cybercrime markets has sparked an abundance of components. Of importance here is the way in which market actors evaluated each other’s skill, knowledge and commitment to technology. These are intrinsic elements of hacker culture, and have clearly influenced the cybercrime market culture, as found in chapter five. Apart from the expected behaviour of market actors, I found that the most notable element of the specific market culture of cybercrime markets was that of vouching. It was not only expected that vendors of malware and other cybercrime services would provide voucher copies to be tested by reputable members, it was also the norm for members to vouch for others based on the reputation and skill level they know the other member had in a different community, or based on previous trades. However, the expectancy of voucher copies is the most evident element of specific market culture for another reason; through the reviews of tools and services, vendors get the opportunity to further develop their product. This focus on development and the technological skill of the vendor clearly resonates with that of hacker culture; mastery, skill, and commitment are considered as core values in the literature on hacker culture. These arguments are in thread with Aspers (2011) explanation of specific market culture involving norms (e.g., who pays for lunch) and expectancies (e.g., how people talk) (2011: 94). Providing voucher copies was a norm on AlphaBay, and the language and phrasing of members were expected to meet an unwritten standard. It was through the language that members were able to identify those who knew what they were talking about (i.e., those who were knowledgeable about technology and hacker decorum) and those who did not know what they were talking about and were thus accused of being outsiders; often as law enforcement or just as someone who did not belong in the community because of lacking knowledge and skill.

In addition, there is the inherent need to brag to show off ones work and the damage it causes. This was what I referred to as external reputation, which involves attention directed at a malware from the mainstream media and other Clearnet mediums. This type of attention is both praised and criticised internally in hacker communities because it damages the highly regarded value of secrecy (Jordan, 2008; Thomas, 2002). As was the case on AlphaBay, where most members would praise the vendors getting their product “famous”, whilst a few criticised this kind of attention because it would probably cause heightened attention from law enforcement officials. Accordingly, it is evident that the external reputation was important to many members
of AlphaBay and therefore it is considered as part of the specific market culture of cybercrime markets.

Lastly, the focus of members’ willingness to learn and accumulate knowledge was also of great importance to market actors and thus considered as part of the specific market culture. This is because, even though the expectancy of skill for buyers is low compared to that of the vendor, buyers were still expected to invest time and effort in order to learn how to use (or spread) a program. If someone were unwilling to commit to this, they were instantly flamed and considered as outsiders of the community. Although lack of skill is in many way not accepted in hacker culture, as long as one shows a willingness to learn and develop ones knowledge and skill level, one gains a certain amount of respect. This was also very much the case on AlphaBay, when members showed little interest in learning something and were ignorant of the fact that they needed to invest time and effort in order to make, for example, a malware work; they were deemed too unintelligent to be attempting a “career” in cybercrime. Conversely, members whom admitted to having low skill levels and little knowledge, but were committed to learn and expand their knowledge, were often encouraged to continue their journey and given lessons in different tricks of the trade. In relation to hacker culture, this kind of willingness and commitment is not only highly regarded, but also demanded (Jordan, 2008; Taylor, 1999; Thomas, 2002).

The norms and expectations of market actors are unique to cybercrime markets much because of their origin and influence from hacker culture. Similar traits can arguably be found in other markets (e.g., free samples when you buy over a certain amount in drug markets instead of voucher copies in cybercrime markets), but the cultural value behind these traits are not the same and are therefore unique to the respective markets. On cybercrime markets, these norms and expectations are influenced by hacker culture, and other markets have their cultural influence from other places (see e.g., Sandberg, 2012).

6.3 Widening the perspective

This thesis has held a quite narrow theoretical framework; hence it is essential to link my findings to larger criminological perspectives. Rational choice theory and social learning theory are amongst the traditional criminological theories that have been applied to studies of cybercrime (Holt & Bossler, 2016; Wall, 2001a; Yar, 2013), particularly in regards to hacking, and we can see a clear connection to those theories throughout my findings.
It became increasingly apparent throughout the research that a lot of the activities on AlphaBay were well planned and calculated, meaning that the deviant behaviour fits into the classical criminological perspective of rational choice theory (Cornish & Clarke, 1986). Firstly, getting into the market itself does not happen at random; you have to purposely go looking for the URL and sign-up to join the marketplace and forum. Secondly, the looming threat of scammers and law enforcement is not deterring enough for the risks to outweigh the perceived benefits of engaging in cybercrime markets. Thirdly, for many of the goods and services to be worthwhile, one has to commit to spend time and effort into using and/or spreading the product. All of these elements point towards a rational actor deciding to engage in deviant behaviour (Cornish & Clarke, 1986). Furthermore, it has been suggested that the motivations behind cybercrime are rational. By this it is meant that crimes are committed because of the rational motivations of the offender, for example monetary gain, curiosity, or revenge (Grabosky & Smith, 2001 in Yar, 2013: 34). Monetary gain is the strongest connection to the findings of this thesis, as the focus on buyers not being skilled was often advertised as making “easy” or “quick” money. There were also some instances where the motivations of members seemed to be revenge, but monetary gain was mostly the aim.

Hence, applying the concepts derived from rational choice theory in future studies of cybercrime markets could contribute to our understandings of the causations of cybercrime. Rational choice theory is also closely linked to deterrence theory (Holt & Bossler, 2016), and therefore by applying rational choice and deterrence theory to future studies on cybercrime markets and forums could provide new insight as to how to deter people from engaging in this deviant behaviour.

In addition, some of the findings of this thesis fit into the positivist criminological perspective of social learning theory (Akers, 1994), which has been tightly knit with studies on hacker culture (Holt & Bossler, 2016: 83; Yar, 2013). The findings from this thesis, however, suggest that the market actors have purposefully sought out AlphaBay with the intention of buying goods or services for malicious purposes. Yet, there could have been members who started out by just being curious of cybercrime tools and services that escalated their involvement through differential association (Akers, 1994; Holt & Bossler, 2016). It is fairly obvious that the AlphaBay forum is a place of learning, and therefore pointedly dismiss the application of social learning theory in the studies of cybercrime markets would be ignorant. Rather, my research further underlines the important aspect of learning that exists in deviant communities online. As I have already showed, when market actors who had little or no knowledge of cybercrime tools
and services, the skilled members were quick to offer advice and guidance in order to teach them how they work. It is also in the socio-cultural environment of the AlphaBay forum that new members to the community socialise and learn proper decorum and become part of the collective, which is also how hackers learn their values, norms and beliefs (Yar, 2013: 38).

I encourage future researchers to enquire into the affect social learning might have on market actors: do they increase their transgressions after being emerged in the world of the cybercriminal? Do they desist from cybercrime after “having a taste”? Answering these questions could perhaps increase our knowledge of the motivations of true cybercrime offenders, especially the less skilled ones who make up the largest number of transgressors (Holt et al., 2012).

6.4 Conclusion

Legal markets are regulated and enforced by the state, and market actors have the possibility of legal recourse if the actor at the other end of the contract fails to uphold their end of the deal (Aspers, 2011; Beckert & Wehinger, 2012; Fligstein & Dauter, 2007; Granovetter & Swedberg, 2001). This regulating force ensures stability, insurance, and transparency on legal markets. Illegal markets, on the other hand, have to imitate the mechanisms of legal markets in order to be efficient and successful. My analysis of the structural features and mechanisms of enforcement on AlphaBay furthers the already established important elements of trust, reputation, and regulation in online illegal markets. In a fundamentally anonymous and secretive environment, such as the Darknet, trust is a vital element for both sellers and buyers. In this thesis, the formal mechanisms feedback system and vendor- and trust levels emerged as the best indicators of someone’s trustworthiness. This has also been found in other studies on online markets, legal and otherwise (Allodi et al., 2015; Ablon & Libicki, 2015; Bakken, 2015; Bakken et al., unpublished; Hardy & Norgaard, 2016; Holt, 2012; Holt et al., 2016; Lacson & Jones, 2016; Radianti, 2010; Wehinger, 2011). In addition, the informal mechanism of reputation also served as an incredibly important indicator of trustworthiness. Trust and reputation are, in other words, tightly intertwined. Market actors cannot have one without the other; you cannot be trusted without a good reputation, and you cannot achieve a good reputation if you are not trustworthy. This is an important point to make, because, as previous researchers also have pointed out, it is here law enforcement efforts can disrupt market stability and efficiency (Holt, 2012; Holt et al., 2016; Lacson & Jones, 2016). By disrupting the reputation and trustworthiness of market actors,
especially “the elite”, one can sow a seed of doubt in other market actors and thus disrupt the efficiency of these mechanisms.

Furthermore, the regulating mechanisms implemented on the marketplace show that the administration put effort into tackling problems of coordination. These mechanisms ensured order and stability to the market. By implementing rules, hiring staff, and enforcing punishment mechanisms on those who transgressed the rules, the administration showed sophistication and efficiency in regulating the market. In addition, market actors could enforce their own regulating mechanism by Blacklisting other members, file scam reports, and publicly expose someone if they had wronged them (e.g., through the feedback system or on the forum).

These findings support the arguments of other researchers and research organs that online illegal markets are rapidly developing and becoming more sophisticated and efficient (Ablon & Libicki, 2015; Allodi et al., 2015; SOCTA, 2017). AlphaBay was the largest and longest running Darknet market when it got shut down, consequently the structural features identified both on AlphaBay and in the existing literature will most likely appear in new markets emerging online, which will ensure order, efficiency, and transparency on the marketplace. As Aspers (2011) explained: ‘a general market culture […] spans many markets and […] can be called into action when people act and when markets are made’ (2011: 94).

In addition to the structural features of AlphaBay, this thesis also looked more closely at the specific market culture of AlphaBay in order to gain a deeper understanding of how market actors related to one another and which norms and beliefs they value. This was done by analysing the influence hacker culture had on the market culture, which lead to some interesting findings; not only did I identify elements of a unique culture of cybercrime markets, but I also found indications of a layered specificity of market cultures (Figure 19 above). Market actors were constantly evaluating other member’s behaviour and language in order to determine whether or not they were insiders or outsiders of the collective community of market actors. This is something that is done by market actors in different kinds of illegal markets, as the possibility of getting caught by law enforcement is a constant risk factor. Therefore, I argue this is part of a broader specific market culture of illegal markets, not just those operating online. However, I did also argue that their evaluation of insiders and outsiders are unique to each market. For example, market actors of drug markets in the physical world analyse other people’s behaviour in order to identify sellers and buyers, as well as possible law enforcement officials (see Sandberg, 2012). On cybercrime markets, I found that they evaluate other market actors based on their relationship
with, commitment to, and mastery of technology, which is also at the core of hacker culture (Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999; Thomas, 2002; Wall, 2001; Yar, 2013).

Further, it became apparent through my analysis and previous research that there are some elements that are part of a broader specific market culture of online illegal markets; namely masculinity and flaming. The anonymous online environment perpetuates hegemonic masculinity (Connell, 1987), and AlphaBay was a prime example of this. There were constant underlying masculine tendencies throughout the marketplace; most obviously displayed in the language (e.g., by use of male pronouns). Particularly the method of flaming showed the more extreme display of masculinity by use of misogynistic language. Because this has been identified in the literature as a vice of anonymity (Jordan, 2008; Jordan & Taylor, 1998; Taylor, 1999) it is highly likely, even expected, to be found in other online illegal markets. Flaming is arguably the element of specific market culture that stands in starkest contrast to general market culture. In most markets, particularly in the physical world, flaming another market actor would in all likelihood be frowned upon, and perhaps even result in some sort of reprimand. Yet, on AlphaBay it was just part of the way they responded emotionally to something they considered as stupid or unfair.

The most apparent and direct influence hacker culture had on the market culture of cybercrime markets were the elements of development, technical finesse, knowledge, and skill. The members of AlphaBay were largely fixated on these elements, and thus they were also under constant scrutiny. If a vendor could not explain their code or teach others how to use their software, then they were deemed fake and unskilled. Knowledge and skill were of great importance on AlphaBay, as in hacker culture, and if one did not possess these qualities one were labelled ‘noob’ or ‘script-kiddie’. Although these labels have innately negative connotations, they were not necessarily frowned upon by other market actors. Rather, as long as they expressed willingness and commitment to learn, they were embraced and welcomed by receiving tips and tricks of how to use and spread the tools distributed on AlphaBay. This shows that even though skill is an essential part of hacker culture and a way for hackers to distinguish between those who are worth their time and those who are not, on AlphaBay it was just considered as the starting point of a cybercriminal career. In fact, most listings for malware on AlphaBay were advertised as being “noob friendly”. This lowered skill level amongst users of cybercrime tools and services has been a cause of concern for academics, computer security experts, lay persons, and law enforcement agencies in recent years (Holt et al., 2012; SOCTA, 2017), and my findings further add to these concerns. Cybercrime tools and services are no longer just accessible to, and
operational for, technological ‘whiz kids’; now they come with full customer support available 24/7 to anyone, at any technological skill level.

To conclude, this thesis has answered the aim and objectives for the study as comprehensively as possible within the decided theoretical framework. I have explored the overall structure of AlphaBay, from the process of becoming a member to understanding the formal and informal mechanisms implemented to regulate the marketplace. I have thoroughly analysed the influence of hacker culture on cybercrime markets. Finally, I have examined the display of general market culture and identified a specific market culture of cybercrime markets. By incorporating economic sociology in the study of cybercrime markets, I have shed a new light on the cultural aspects of these markets. The distinction between general market culture and specific market culture proved to be a fruitful perspective in order to understand the social, and thus economic, behaviour of market actors. This thesis, therefore, complements the existing literature on cybercrime markets, and broadens the understanding of other online illegal markets by proposing a layered specific culture of these markets.

Word count: 35 462

Excluding summary, acknowledgements, table of contents, footnotes, bibliography and appendix.
Bibliography


TorProject (2016) ‘About Tor’ [online] Available at: https://www.torproject.org/about/overview.html.en (Accessed 10.03.2016)


Appendix

1. Screenshots

1. Screenshot of the Administration announcing the implementation of ‘ScamWatch’:

The anti-scam team, ScamWatch, is a paid position and consists of @vass and @onionhood. Each member is proven and recognized, each with individual focus - not only fraud but drugs, hacking, malware, general etc. Staff has long worked to prevent scammers, however, with the increase of user base, we needed a team to entirely focus on detecting and preventing scams of any sort.

Staff is part of ScamWatch programme and will follow same procedure with the difference of being able to moderate topics/delete listings/make products physical etc. ScamWatch members at current stage do NOT have any moderation permissions on the forum or dispute access in marketplace.

What do ScamWatch members do?
They patrol all the time AlphaBay marketplace and forums to detect/prevent scams or signal for potential ones. ScamWatch members will have the ability to freeze vendor account withdraws for 24hrs if suspected of scamming. Issues such as physical items marked as Digital (scam) will be enough for freeze and report to Administration.

Example ScamWatch procedure?
After an account is frozen, SW member/Staff responsible for it will create post in hidden forum section, explaining the situation (+details+evidence) and Administration will be able to apply ban within 24hrs or dismiss the case, e.g. due to lack of evidence.

2. Screenshots explaining the role of the Notarius

*Multi-Trust Contracts* are identical to normal Contracts with the difference that in case of dispute, a 3rd-party will handle your dispute - appointed by the community "Notarius" members ([URL](https://en.wikipedia.org/wiki/Notarius#URL)). Notarises will have the same function as moderators who are dispute resolvers with the difference that Notarises will solve only cases (Contracts) they have been assigned to during creation of contract by the user.

The "Notarius" group will consist of high-ranked & trusted members which have been active and useful for the community. To join, you have to be known (several months active) in an area of use to the community in some way.

3. Screenshot of GRB function:

After a long process of selection and sorting, we have settled on the best possible candidates for GRB in its current state. We have concluded a full rebuild of GRB is required, first by unapproving all GRB guides (including the old ones which are still with the tag Verified by GRB) and second by introducing some changes including thorough review of all guides posted, having the free help of GRB members to improve/upgrade your guide, as well as general selection process security measures to ensure only *quality* is synonymous GRB and its work.

Previously GRB was merely used as a tool to filter out poor guides but as the community has evolved and showed it is not enough so must the board evolve and its processes. Now, we see GRB to have a great opportunity to shape the 'guide selling' sector and put an end to the bad selling practices of any kind. For the future as previously mentioned, we see GRB to play key role in selecting the best and attaching its name only to those guides which truly pass the test and are working, which in turn would restore peoples faith in GRB and its work.
100

4. Screenshots from the administration’s tips on how to stay anonymous and not get caught:

If you are new to the Darknet Markets, there are some basic steps you must take in order to prevent LE (Law Enforcement) from getting to you. Some of you might say, “I am just buying a gram of weed to I am not a big target”, but you never know when LE will have less work and will start to prosecute smaller cases. Always assume that you will be under investigation and act accordingly. Being able to sleep quietly at night and not having to worry about police every time someone knocks at your door is definitely something enjoyable.

We recommend that you do not follow the advice regarding personal security found in the carding guide made by alphaz (former admin retired in Aug 2013). It was imperfect oops and using Windows is never a good idea, regardless of your firewall settings. We will get to it later.

1) Never use a username that you use on the clearnet. It should go without saying, if a simple Google of your username can lead to your Facebook or any clearnet profile, you’re in for some deep trouble.

While this isn’t court admissible evidence, it gives a starting point for LE, which could lead to your conversations being monitored, bank accounts looked at, etc. For example, the current admins only use “Admin” as a screen name. This obviously isn’t tied to any clearnet profile. If you are currently using an account with the same username as a clearnet profile you use, you should change it. You can also find an account on the clearnet and use this username if the account isn’t yours, to “set up” someone, but this is not recommended and can have risky consequences.

2) Stay away from Windows. If you really need to use Windows for other purposes, then have a dual boot with Windows and a Linux distribution used for illegal stuff.

We highly recommend Qubes OS as it offers added security. If for some reason Qubes can’t fit on your system, most Linux distributions will do, as long as you set your privacy settings correctly. On Windows, LE can send you a special update that will monitor what you are doing. Microsoft plays ball with U.S. Law Enforcement. In fact, you should completely stay away from everything that isn’t open source if you are looking for perfect security, as you never know what backdoors might be there.

3) Use encryption whenever possible. Most Linux versions come with LUKS encryption, so you should make use of it and use full disk encryption.

Then, inside your Linux partition, put all your illegal stuff inside a TrueCrypt container. There are 2 programs who can achieve this correctly, and they are TrueCrypt 7.1a and VeraCrypt. Both are backdoor-free. Create a hidden volume inside your volume, where you will put all your illegal stuff. In your outer volume, put sensitive things that you want to hide from prying eyes but that you have no problem with LE seeing, such as nudes, bank statements (if not incriminating), tax reports, etc. If you are forced to reveal your password, you will be able to give the fake password (opening the outer volume) and have a perfectly good reason to justify why you are using encryption. While in, USA, the police can’t force you to surrender your password, they can hold you in custody and make the procedures stall without moving, until you suddenly remember your password. Forensic analysis has proven that it is impossible to prove that a hidden volume exists in your TrueCrypt container. Take advantage of this, and respond with “unsure, officer” when asked for your password, which will obviously be your outer volume password.

4) Put your illegal stuff in a VM. Many applications will leave log files, cookies, temp files, or traces that can very tedious to cleanly manually without leaving a single trace.

Plus, there’s hard drive recovery that can find the traces. Use a VM like VirtualBox or VMWare, and put all the illegal stuff inside that VM. Do absolutely nothing illegal outside that VM. Put the VM files inside your TrueCrypt or VeraCrypt hidden volume. Once the VM is shut down and the hidden volume dismounted, all the proofs are gone. You don’t want to risk getting a cookie of a file in your temp folder that rings a bell.

5) Use Bitcoin tumblers. There is a major difference between “tumbling” coins, and “moving coins”.

No matter how many times you send your Bitcoins to another wallet, cut in half, send to 2 wallets, resend, etc. there are special investigations tools that can follow the trace and find exactly where your coins went. If you send the coins to an exchange anonymous account, convert to Litecoin, send to another exchange, convert to BTC, and send again, LE can subpoena all those exchanges and get the in/out addresses and still trace you. While blockchain analysis has never been used to convict someone (nor is it court-admissible evidence), it gives an interesting entry point for an investigation. Tumbling coins means sending the coins to a tumbling service (see your Balance page for a list), waiting a few hours, and withdrawing. Everybody mixes their coins in the pool, so you actually receive someone else’s coins. Unless LE has access to the tumbler’s database, the trace is broken and it is unbeatable.

To put an end to the never-ending debate regarding “does tumbling work”, we are Bitcoin experts and know all the protocol in its details, and we answer with a clear “yes, it does”. It’s simple: if you send coins to an address, and then receive coins from that address, the coins come from a completely different source without any trace to the previous address, no forensics tools in this world can find you. It’s just impossible, as the trail does not exist. The only link is in the website’s database, which gets purged after a few days. You just got the coins from someone else. That’s the reason why taint analysis isn’t admissible to court: there are just too many possible reasons as to why you get “those” coins.

6) Use a drop for physical stuff. If you order drugs or use a stolen CC to card some goods, always ship the items to a drop that isn’t related to you.

Drive around your neighborhood and find such a place, this shouldn’t be hard. Do not send drugs to your home address, nor carded goods, ever. Also, refrain from using a friend or relative’s house as a drop. It must be unrelated to you. If someone asks if you are expecting a package, always say no. If you mistakenly ordered something to your home address, write on the package “return to sender” and let it sit near the door for a week or two. This will help if you get a controlled delivery (CD). You might receive a package without issues, but be on a “watch list” and get raided next time. You never know if you’re being spied on, so assume the worst.

7) Do not brag about what you are doing. After a while on the Darknet, it is possible that you might start making enough money to make some people jealous.

Keep a low profile and do not brag about it. It may sound harsh, but in your everyday life, most people silently want you to fail so they don’t feel left out. A secret is best kept by yourself only. How many time have you seen someone starting getting successful, and felt some jealousy and wanted this person to fail so you didn’t feel “left out”? Be careful with that.
8) Use a VPN with Tor and bridges. Never trust your VPN, even if it claims to have no logs.

You can ask Tluiec if he thought HideMyAss was a good VPN or not. They straight out handed his information to law enforcement. You should use bridges to access Tor, and send all that traffic through your VPN. This way, in order to catch you, all 3 elements will need to be compromised. Don’t be lazy on security. Change bridges on a weekly basis, change VPN provider often. Also, we highly recommend disabling JavaScript while browsing the Darknet, as there are some zero-day exploits that may reveal your IP or perform any unwanted behavior. IP trace is a good proof against you, so don’t let your enemies obtain it.

9) Never reuse passwords. Many people get phishing on Alphabay because they got phishing on another site and were using the same password.

Also, if LE has a doubt about you and knows one of your passwords, they can try it on your Darknet accounts, and also ask your daily life sites to turn over your password, as it isn’t always one-way encrypted. If they logged in your Alphabay with the password "iLoveCats323" and your Facebook password is "iLoveCats494", the link is pretty easy to make. You should use long and complicated passwords, and keep absolutely no pattern between all your passwords. Passwords being one-way hashed means nothing; there are keyloggers and malware out there that will quickly make hashing useless.

10) If you get arrested, KEEP SILENT AND CONTACT A LAWYER ASAP. The police get years of training on how to make a suspect talk, promising you a reduced sentence, just "trying to prove that you aren’t guilty so they can leave you alone", they will try to make friends with you, trying to connect with you and make you feel comfortable. The truth is, this is bullshit and they can lie whenever they feel like it. They have 1 goal: make you confess, directly or not. If you get arrested, kindly say "I understand you are doing your job officer, but I prefer to remain silent without my lawyer". Do not fall for their promises, kindness, etc. as it is all a show. Contact your lawyer and let him take care of this for you. This can probably means a few days in custody, but you’ll save yourself some precious months (or years) in prison. Check the Youtube video "never talk to the police" for the full information on why you should always keep silent.

There is no perfect opsec in this world, but those 10 tips will definitely increase your security to a point where you are extremely unlikely to be found. There are several other factors to pay attention to like stylometry, location markers, language dialect, bank activity, etc. but those 10 tips alone should discourage LE from pursuing you unless you are a very high profile target. Encryption (...) is the most important one. The encryption keys are stored in RAM. This makes sure that whenever LE enters your house, your "criminal enterprise headquarters" (computer) becomes an inoffensive machine without any evidence.

And to add to all that... It might sound self-explanatory, but many people do not seem to understand that: Do not get phisheled! We have no pity for those who get phished, and you just compromised all your customers and partners. Do not get phished, ever.

5. Screenshot from AlphaBay FAQ [Frequently Asked Questions]:

1. What is Alphabay Market?
Alphabay Market is a marketplace founded by reputable members on Russian carding forums, and transferred to new administrators in May 2015 in order to make better plans for the future growth of the market. We are a darknet market that specializes in all kinds of illegal goods.

6. Screenshot from the forum showing the administrator’s signature in Russian and English:
7. Screenshot of Admin explaining the purposes of choosing Trust Levels:

*Vendors* can now select a visibility level range with their listings, when editing it. Buyers outside that trust range will not see your listing. For example, if you are vendor Trust Level 5, you can set your listing to be available to see only to buyers who are Level 5 or above. This serves 2 purposes:
- Keep LE away by making infiltration harder.
- Make special deal with the high rollers here.
(by default, your listings are visible to everyone, unless you manually change this value as a vendor).