UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL SCIENCE AND ENGINEERING

School of Electronics and Computer Science

Deviating from the cybercriminal script: Exploring the contextual factors and cognitive biases involved in carding

by

Gert Jan van Hardeveld

Thesis for the degree of Doctor of Philosophy

September 2018

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL SCIENCE AND ENGINEERING

Web Science

Thesis for the degree of Doctor of Philosophy

Deviating from the cybercriminal script: Exploring the contextual factors and cognitive biases involved in carding

Gert Jan van Hardeveld

This thesis explores the contextual factors and cognitive biases involved in the decision-making of carders. Carders engage in carding, the obtaining and cashing out of stolen payment card details. This works examines what operational security carders employ to stay secure and how they can make mistakes in these processes. It also analyses what mechanisms are in place to create bonds of trust in pseudonymous environments on the Web and how this complicates investigations into such illicit activities. Tutorials, created by carders, are analysed with crime script analysis to create insights into 'optimal' decision-making and to design situational crime prevention measures. An analysis of the organisation and tasks involved in carding with the CommonKADS method, however, will show that more extensive mapping of the carding process is required to understand decision-making. Cognitive biases will be explored to better understand the psychological reality of online crime commission. Expert interviews with law enforcement officers, bankers and card issuers will provide some evidence for the existence of such biases in carders. These interviews will also create novel insights into tactics against carding and common issues encountered in policing such international online crimes.

Table of Contents

List of Tables

List of Figures

Academic Thesis: Declaration Of Authorship

I, Gert Jan van Hardeveld, declare that this thesis entitled

Deviating from the cybercriminal script: Exploring the contextual factors and cognitive biases involved in carding

and the work presented in it are my own and has been generated by me as the result of my own original research.

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:

    - van Hardeveld, G.J., Webber, C., Hooper, C., Middleton, S.E. & Surridge, M. (2015). The Digital Police Officer: Using Natural Language Processing to Identify Cybercriminals. In *Proceedings of Eurocrim*, 143.
    - Webber, C., Hooper, C., Middleton, S.E., Surridge, M. & van Hardeveld, G.J. (2015). The Pleasures and Pains for Transdisciplinary Research for Criminology: Insights from

the Digital Police Officer Project. In *Proceedings of Eurocrim*, 285-286.

- van Hardeveld, G. J., Webber, C., & O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. In Proceedings of *Workshop on online safety, trust and fraud prevention. ACM Web Science Conference*, 1–5.
- van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244–1266.
- Van Hardeveld, G. J., Webber, C., & O'Hara, K. (2018). Expert perspectives on the evolution of carders, cryptomarkets and operational security. In *Proceedings of the Evolution of the Darknet workshop*, 6-10.

Signed:

Date: 30-08-2018

Acknowledgements

> "Hanging on in quiet desperation is the English way"
>
> - Roger Waters (1973)

Unfortunately for my friends, family and supervisors, I'm not English and my desperation has thus not always been very quiet. Therefore, I want to take the chance here to thank several people for their patience and support.

First of all, I would like to thank my supervisors: Craig Webber and Kieron O'Hara. Craig has been my supervisor since my master's thesis. He let me join the *Digital Police Officer* project and, most importantly, introduced me to various aspects of criminology. His aversion to rational choice theories and administrative criminology helped me to clarify my research and focus on the aspects of carders' decision-making that matter. Kieron came on board halfway through my PhD and helped me in adding focus and structure to the PhD by introducing me to CommonKADS. I also would like to thank Tim Chown, who supervised me during the master's thesis and in the first half of my PhD, before he left the University.

Of course, I would also like to thank the Web Science Centre for Doctoral Training, particularly Susan Halford, Les Carr and the programme managers. The iPhD, and the opportunities that came with it, has been amazing. Writing retreats, summer schools and networking trips have taken me from Windsor Great Park to Singapore to the San Francisco Bay Area to St. Petersburg, for which I'm very grateful. Also, I would like to thank all the other Web Scientists from various cohorts who have become my friends and made me feel at home in Southampton. The sports we have played and beers we drank in Stag's have been necessary distractions and helped me keep my sanity.

Parts of this research could not have been completed without TNO providing me access to their tool the *Dark Web Monitor*, for which I am grateful. I would also like to thank all the interviewees who have participated in this study. The insights into their expert knowledge and experiences have been invaluable and massively helped my research.

The last four years have been mostly great for me. I have enjoyed doing the PhD, interning at INTERPOL in Singapore and exploring this interesting field of study in the UK and around the globe. Also, I was lucky enough to meet Emer, my partner in crime, who I would like to thank for her continuous support, humour and love.

Finally, I would like to thank my family, especially my parents. Over the last four years we have been through some sad times, in which we lost close family members: Oma van Hardeveld, Opa van Steenis and Kees. Being in another country has not always been easy at such times for me, but I’m very grateful that, no matter where I was, my family have always provided me with their support.

Chapter 1 Introduction

> "In a closed society where everybody's guilty, the only crime is getting caught. In a world of thieves, the only final sin is stupidity."
>
> - Hunter S. Thompson (1972)

1.1 The relevance of studying online card fraud

Over the last three decades, the Web has brought many advantages to the world by augmenting global peer-to-peer flows of information. Blogging, social networking and e-publishing platforms are some examples of Web-enabled mechanisms that have given individuals access to information on unprecedented levels. However, the omnipresence of information on the Web has also amplified chances for existing and new crimes to be executed on a much larger scale than ever before. These can be characterised as cyber-enabled (or cyber-facilitated) and cyber-dependent crimes. The first are crimes that already existed before the Web, but are now also facilitated by it, such as card fraud, the illicit drug trade and arms trafficking. Cyber-dependent crimes exist because of computer networks and other forms of information communication technology (ICT). Examples of cyber-dependent crime include the spread of malware for financial gain, distributed denial-of-service (DDoS) attacks to cause (reputational) damages, and hacking to steal payment data (NCA, 2016; Europol, 2017). Due to the advent of the Web, complex tasks can be executed on a global scale. This has enabled both individual offenders and organised groups to acquire skills for committing online crimes, to find individuals with these skills to 'outsource' tasks and to find victims on a global scale (Wall, 2005; Yip, Shadbolt & Webber, 2013; Levi, 2008). This thesis has particularly focused on one type of cybercrime for which the changing nature of crime into the online realm has been important: carding.

Carding traditionally referred to the illicit use of stolen payment card details, both credit and debit, to obtain stolen goods and services. However, over time, the term has changed to include all activities involved in stealing the payment details and cashing them out as well (Peretti, 2009). Individuals involved in the trade of stolen payment card details, i.e. carding, are referred to in this work as *carders*.

Carding is mainly a cyber-enabled crime, as fraud with credit and debit cards already existed before the existence of the Web. However, carders sometimes also obtain payment card details by, for example, spreading malware or hacking. This makes offenses related to the carding process partly cyber-dependent as well. Carding is commonly distinguished into two types of fraud: card-present (CP) and card-not present (CNP). With card-present fraud, offenders have to be in the possession of a physical card. The payment card can either be physically stolen or copied through skimming at automated teller machines (ATMs) or point-of-sale (POS) terminals, after which data from the original card is copied onto counterfeits. Carders can then try to cash-out at an ATM or POS terminal (Europol, 2017).

Card-not present payments are payments via Internet, post or telephone without the physical presence of a credit or debit card (ECB, 2015). CNP fraud thus does not require the presence of a physical card, as a carder only needs to obtain the details on the payment card of a cardholder to fraudulently use them. Carders often obtain card data through data breaches at businesses or through online phishing Thomas et al. (2015). While the acquirer of card data could immediately cash the cards out, they often end-up for sale on marketplaces and forums. Some argue that this occurs, as the quantity of data in the possession of small groups of hackers is generally too big to use without risking detection (Holt, Smirnova & Hutchings, 2016). This work primarily looks at CNP fraud. However, as will be shown later, CP and CNP overlap in some cases.

CNP fraud has in recent years seen a growth in size, as is shown below in Table 1.1. Next to visible statistics, i.e. the fraud that has been reported, the unreported and thus not visible part of CNP fraud is also assumed to be large (Europol, 2017). It is also likely to grow more in the future, as CNP payments are increasing and old payment cards prone to counterfeiting are slowly being replaced globally by new technologies, which makes card-present fraud less appealing for carders (Hayashi, Moore & Sullivan, 2015). On the contrary, ATM and POS fraud decreased with 50% from 2008 to 2013 in the Single Euro Payments Area. The increasing global adoption of chip and pin, skimming device detectors, lids to shield PIN and other improvements on the design of ATM card slots have contributed to this (ECB, 2015). The fact that CNP fraud happens without the presence of a card makes physical protection harder. CNP fraud is likely to grow if no new effective countermeasures are implemented (ECB, 2015). The size and probable rise of CNP fraud make research looking into how card details are abused and what can be done about it necessary.

The most recent official statistics for the entire Single Euro Payments Area have shown that CNP fraud made up 66% of all card fraud in 2013. This amounted to a loss of 958 million euros, according to the European Central Bank (ECB, 2015). In the United States, the UK, South Africa and Australia, CNP fraud has also become more prevalent, relatively to other fraud types, as can be seen in Table 1.1 below. These countries were selected, as card fraud statistics were obtainable from government-issued reports. Continental, or even national, government-issued reports with statistics on card fraud from countries in Latin America, Asia and Africa, with the exception of South-Africa, seemed to be not publicly available in English. However, there are some statistics available from industry. It is estimated that card fraud in Asia in 2014 cost the Asian pacific region US$360 million to $420 million per year. Also, a rise in CNP was observed[1]. While official government-issued statistics are lacking, business reports do state that CNP fraud is becoming more prevalent in Latin America as well[2]. It must be noted that cybercrime statistics, from government, industry and academia, are often not fully accurate, because of several hurdles to accurate reporting and various interests that affect such representations (Hyman, 2013; NCA, 2016; Cross, Richards & Smith, 2016; Harrell, 2015). Still, reports overall show there has been a global trend that CNP fraud has been on the rise.

Sometimes the fact that CNP fraud is going up is reflected in absolute numbers, but not in relative percentages. For example, in the UK in 2015 CNP fraud amounted to £398.2 million. In 2016, this was £432.3 million, an increase of 9% overall and 18% for e-commerce specifically (Financial Fraud Action UK, 2017). Still, the percentage in comparison with total card fraud stayed the same compared to 2015. Similar trends were visible in South Africa and Australia from

[1] http://www.cio-asia.com/tech/internet/cnp-fraud-costs-apac-banks-more-than-us350-million-annually-fico/

[2] http://www.wincor-nixdorf.com/internet/cae/servlet/contentblob/1305402/publicationFile/86553/Whitepaper.pdf

2015 to 2016, where absolute numbers of CNP fraud increased, but relative numbers decreased slightly. CNP has thus not become less prevalent in 2016, but other types of fraud have increased relatively even more than CNP. The available government-issued statistics on CNP in the USA in 2015 were much lower than in the UK, Australia or South Africa. This can be explained by the fact that the USA is slow in adopting Europay, Mastercard and Visa (EMV) chip technologies and thus suffers more from card-present fraud than countries who have adopted EMV, which will be further explored in Chapter 7.

Percentage of CNP of total card fraud	Europe	UK	USA	South Africa	Australia
2016	?	70[3]	?	67[4]	78[5]
2015	?	70[6]	39[7]	75[8]	79[9]
2014	?	69[10]	?	42[11]	78[12]
2013	66[13]	67[14]	?	49[15]	72[16]

Table 1.1 Percentage of card-not present fraud in relation to total card fraud

This research has specifically focused on online CNP fraud. Not all CNP fraud occurs online, as postal or telephone fraud can also be classified as CNP. However, it is a significant percentage and likely to go up in the future, as many payment infrastructures move to the online realm. For example, e-commerce or Internet fraud in the UK took up 66% of total CNP fraud in 2014 and 2015. This

[3] Financial Fraud Action UK, 2017
[4] SABRIC, 2017
[5] Australian Payments Clearing Association, 2017
[6] Financial Fraud Action UK, 2016
[7] Federal Reserve, 2016
[8] SABRIC, 2016
[9] Australian Payments Clearing Association, 2016
[10] Financial Fraud Action UK, 2015
[11] SABRIC, 2015
[12] Australian Payments Clearing Association, 2015
[13] ECB, 2015
[14] Financial Fraud Action UK, 2014
[15] SABRIC, 2014
[16] Australian Payments Clearing Association, 2014

respectively amounted to £217.4 million and £261.5 million, which were the highest numbers measured since data collection began (Financial Fraud Action UK, 2014, 2015). These are a considerable burden on a wide array of parties, such as consumers, merchants and banks.

Carders sometimes justify their actions by arguing there is no harm for the cardholder, because reimbursement will occur (Yip, 2016). While this might be true in some countries, there have been public calls to make cardholders more responsible in the future, such as by the UK's Metropolitan Police Commissioner in 2016 (Loveday, 2017). More card fraud will put more financial strain on banks and merchants, which could lead to larger societal financial problems and lack of trust in financial institutions. Therefore, examples of stakeholders in online card fraud will be discussed below, to get a fuller picture of what effects carding can have on society and why it is relevant to study its effects, organisational structure, tasks, its agents and their operational security.

Roles	Categories	Stakeholder examples
Payment data holders	Victims	- Cardholders (individuals and companies) - Merchants (airline, car rental, hotels, ecommerce platforms etc.) - Banks, card issuers
Infrastructure providers	Payment service providers Proxies Cryptocurrencies Cryptocurrency exchanges Cryptocurrency mixers Online payment providers and other services used for laundering	- IDEAL, WebMoney, Skrill - VPNs, VMs, SOCKS, RDP, Tor - Bitcoin, Litecoin, Monero - ShapeShift, CoinBase - CoinMixer - PayPal, freelancer.com, Ticketmaster, gift card websites, etc.
For-profit protectors	Banks Card issuers Security consulting	- HSBC, Wells Fargo - PayPal, Mastercard - PWC, Accenture
Public protectors	Law enforcement (national) Law enforcement (international)	- FBI, NCA - Europol, Interpol

Table 1.2 Stakeholders in online CNP fraud

This work bases the above stakeholder classification on Sheng et al. (2009) and thus divides stakeholders into *payment data holders*, *infrastructure providers*, *for-profit protectors* and *public protectors*. *Payment data holders* are the parties that suffer direct losses from CNP fraud. *Infrastructure providers* are the parties that are used by carders to illicitly obtain profits from stolen card details and to launder these funds, as securely as possible. *For-profit protectors* are companies that sell solutions or provide consultancy against online crime to *payment data holders* and *public protectors*. Banks and other card issuers can be both *payment data holders* and *for-profit protectors*, as they provide solutions to minimise fraud from which they make profits and get new customers, but they also feel the financial consequences of fraud. *Public protectors* are national and international law enforcement agencies that have the task to fight online fraud and prosecute individuals who perpetrate such acts. CNP fraud is a primary concern for *payment data holders* and *public protectors*. This is the case, as *payment data holders* are the ones who lose money when it comes to online fraud. *Public protectors* are often charged with solving such cases.

On the contrary, *infrastructure providers* and *for-profit protectors* will only get involved in solving CNP fraud if there is a monetary incentive. Some *infrastructure providers* will only help *public protectors* solve CNP fraud if ordered to do so in a court order, as sharing data from their company might contrast with their business philosophy. *For-profit protectors* will only help clients who pay for their services. This work tries to touch upon all four groups to address the issue of carding in an inclusive manner. It addresses how carders obtain funds from the stolen payment details of *payment data holders* and how this can possibly be minimised. *Public* and *for-profit protectors* were interviewed in this regard. Also, one *infrastructure provider* was interviewed. Explanations of what *infrastructure providers* are and the manners in which they are misused for CNP fraud are extensively discussed throughout this work, particularly in Chapter 4 and Chapter 5. These four groups represent the various stakeholders in carding. However, carding has also been a part of a larger trend of cybercrime. Therefore, below, the evolution of carding in the context of cybercrime will be explored.

1.2 Carding in the cybercrime context

The term *cybercrime* has been used to indicate a wide variety of crime types. According to Wall (2001, p. 2), the term signifies “a harmful behaviour that is somehow related to a computer”. Wall stressed that the term has been invented by the media and had no “referent” in law. This changed in the early 2000s, when the first international treaty on cybercrime, the Budapest Convention on Cybercrime (Council of Europe, 2001), was signed to create mutual understanding of what cybercrime entails and to enable international cooperation within a legal framework. Cybercrime has since been a useful umbrella term to describe offences that use some form of networked computer technology. The technical evolution of these networked computer technologies and their social usage is of major interest of much research. Also, the applicability of traditionally ‘offline’ criminological theories to the online environment is something that is widely explored in cybercrime scholarship, as will be shown in 1.3. This research has also examined the applicability of traditional criminological theory to developments in the socio-technical criminal use of networked technologies. The current state of cybercrime, particularly related to carding, is examined below to set the scene for this research.

1.2.1 Evolution of carding

Over the last two decades, infrastructures for the online sale of stolen payment card details have evolved. This has similarly been the case for other types of online crime. Before the prevalence of marketplaces and forums, carders mainly used Internet Relay Chat (IRC) to find channels in which to obtain and sell stolen payment card details (Thomas & Martin, 2006). IRC has been used for online real-time message exchanges on which public and private messages can be sent. Public messages are shown in a channel. Such channels focus on a specific topic, for example #carding or #cc. These are openly accessible public messages. Private messages are sent on a one-to-one basis. These channels and private messages have been used by carders to buy and sell stolen payment card details, amongst other types of illicit goods and services (Franklin et al., 2007).

Systems of reputation and trust could however not be built on IRC, which led to a market where products were generally not of high quality and participants could easily be scammed. Such markets, where it is impossible to verify the quality of trading partners and products, have been referred to as lemon markets (Akerlof, 1970; Décary-Hétu & Dupont, 2013; Yip, Webber & Shadbolt, 2013; Hutchings & Holt, 2017). Therefore, over time, carders moved away from IRC. They moved to public Web forums (Holt & Lampke, 2010). On these, participants could get formal roles and be verified by moderators (Décary-Hétu & Dupont, 2013; Soudijn & Zegers, 2012). Some carding communities even adopted closed forums, which were only accessible after being invited by existing members or paying a fee (Motoyama et al., 2011). With the help of these developments, carders could minimise the risk of being scammed and increase trust in other participants, which is further discussed in 1.2.2.

There are clear advantages for carders in using forums over traditional websites or messaging services. Yip, Shadbolt and Webber (2013) identified four socio-economic mechanisms that explain carders' adoption of forums:

- Formal control and coordination
- Social networking
- Identity uncertainty mitigation
- Quality uncertainty mitigation

Formal control and coordination on a forum, i.e. a hierarchical structure with different roles, can lead to a more regulated environment. Certain users will then have more powers than others and, for example, be able to ban users when they violate the terms of service of a forum. Yip, Shadbolt and Webber stress the importance of social networking for carders, as it is a way for them to obtain necessary skills and resources for their illicit activities. Forums further help in establishing whether a carder is trustworthy enough to trade with. Users use pseudonyms and can thus in principle easily rip someone off without facing consequences. However, allowing forum members to check previous behaviour of a user, such as forum messages and ratings, helps in mitigating this. See 1.2.3 what such mechanisms of trust further entail. The final socio-economic mechanism, quality uncertainty mitigation, contributes to the usefulness of forums, as senior forum members can review the offered products, before a user can become a vendor (Yip, Shadbolt & Webber, 2013; Peretti, 2009). However, since the advent of the first cryptomarket in the early 2010s, stolen payment card details are also being sold on the darknet. Individual focus on operational security measures has changed accordingly.

Since the early 2010s, online marketplaces specialising in the sale of illicit goods and services have frequently made headlines because of the rise of cryptomarkets. These hidden services on the Tor network[17], which are anonymous TCP-services that can be browsed, have become 'sophisticated' environments where users have evolved in ingenuity. Hidden services on Tor are often referred to as 'the darknet'. Buyers and vendors of a wide variety of illicit products and services, such as drugs, child-abuse material, malware, illegal wildlife products, counterfeit products and stolen payment details, use markets on the darknet, as they are a criminal innovation that offers increased (perceived) safety compared to the regular Web (Kruithof et al., 2016; Aldridge & Décary-Hétu, 2014; INTERPOL, 2017). Hidden services on Tor that focus on the sale of illicit products and services and on which cryptocurrencies, generally Bitcoin, are used as payment method are often referred to as 'cryptomarkets'.

Cryptomarkets are markets, often with forums incorporated, on the Tor network or other anonymisation services, such as i2p, on which cryptocurrencies are used for payments (Martin, 2014; Barratt, 2012). Tor uses onion routing, which is an anonymity technology that fragments the links between client and server in various steps by sending traffic through various random encrypted relays. Traffic has one layer of encryption per relay. These layers are then peeled off, hence the onion metaphor, leading to unencrypted plaintext message at the exit node (Reed, Syverson & Goldschlag, 1998). An exit node is the last relay in the chain before the receiver of the message. It can thus observe the content of messages if they are not encrypted by the user, but will not see its source (Li et al., 2013). Tor can be used as a browser that can access normal top level domains (.com, .co.uk, .nl etc.), but also offers 'hidden services' (.onion pages), which are

[17] The technical workings of the Tor network are discussed in more detail in Chapter 5.

only accessible through the Tor network. They do not reveal the IP-addresses of the creator of the hidden service (Dingledine, Matthewson & Syverson, 2004). The technical workings of onion routing are visualised in the graph below.

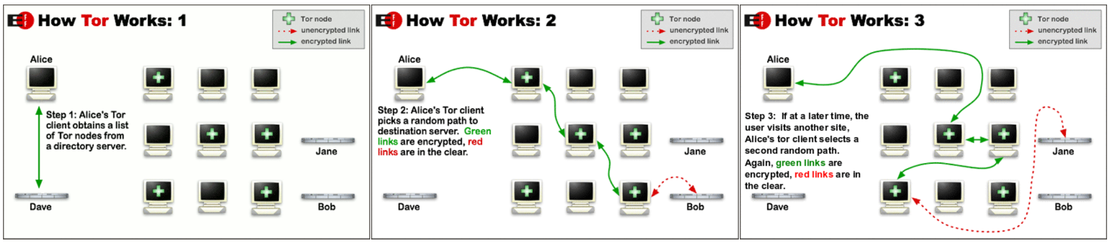

How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob
How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob
How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Figure 1.1 Onion routing[18]

The cryptocurrency most used on cryptomarkets is Bitcoin. Bitcoin is a pseudonymous system that aims to provide more privacy than fully identified payments through banks. Bitcoin was created to allow for direct financial transactions without the intervention of a third party. It also solves the problem of double-spending, with the introduction of the blockchain. The blockchain is a distributed public ledger of all transactions ever made with Bitcoin and serves as a database that checks on double-spending with user's verified signatures (Nakamoto, 2008). A public database of transactions seems to defeat the purpose of privacy enhancement, but the only identifying information is some seemingly random numbers (Hobson, 2013), which include the public key of the payer and payee, amount of Bitcoins being sent and timestamps.

Aldridge and Décary-Hétu (2014), whose research focused on the drug trade on cryptomarkets, have argued that the first cryptomarket was a paradigm shifting criminal innovation. The authors particularly ascribed this to the potential of cryptomarkets to change traditional criminal (drug) markets. Forums and marketplaces thus exist on a continuum from unregulated forum-based markets filled with scammers to maturely regulated and maintained (crypto)markets (Allodi, Corradin & Massacci, 2016). Wall observed in 2001 how the Internet has affected crime by making it more international, allowing communications between offenders engaging in harmful activity and how it separates time and

[18] https://www.torproject.org/about/overview.html.en

space leading to new opportunities for crimes. Cryptomarkets have further augmented these characteristics, as their technical structure and users' operational security complicate law enforcements' investigations even more. This is further explored in 1.2.3.

On cryptomarkets, similarly to carding forums on the regular web, users take up specialised roles for control and coordination, but also, for example, to facilitate transactions. This has been characterised as cybercriminal labour division (Aldridge & Askew, 2017; Thomas et al., 2015; Soudijn & Zegers, 2012). Online crimes generally yield relatively low gains, but occur in large quantities (Moore, Clayton & Anderson, 2009). It is therefore hard for law enforcement to know where to focus on, also because the crimes committed via these markets happen on a global scale. It must, however, be noted that research has suggested that in the drug trade on cryptomarkets increased localisation of product destinations has occurred (Demant et al., 2018). Still, with carding this is less likely to occur, as it does not have similar shipping issues as the online drug trade, because there is no physical illicit product that has to be moved until the cashing out phase. Even if law enforcement has a specific target in mind on cryptomarkets, whether it is one user or an entire marketplace, the technical structure of Tor and the operational security measures taken by members of marketplaces will make it complex for them to be successful in arresting users or closing down marketplaces (Morselli et al., 2017; Moore & Rid, 2016; Soska & Christin, 2015). These operational security measures have also contributed to the fact that cryptomarkets have been a paradigm shifting innovation.

1.2.2 Trust and operational security

Operational security (OPSEC) is a term that originates from military environments. Information leaks about classified operations can help an enemy in their goals. If these kinds of leaks can be minimised, in the military context, lives may be saved (Michnowicz, 2006). OPSEC is therefore in place to create mechanisms that can protect sensitive information and in this manner safeguard secrecy. Next to the military, law enforcement agencies often use OPSEC methods to protect intelligence. In opposition to government agencies, the parties that such agencies are trying to pursue also use OPSEC. For carders, and other cybercriminal communities, OPSEC is a commonly used term to describe the security practices employed to stay safe in the process of trading and cashing out stolen payment card details. Cybercriminals and the platforms they use need to be cautious with their OPSEC methods, as mistakes can lead them to being deanonymised and possibly arrested (Morselli et al., 2017; Ladegaard, 2017; Buxton & Bingham, 2015; Lusthaus, 2012)

The 'classified' information on cryptomarkets that has to be protected by OPSEC measures mainly revolves around the identities of users. They therefore have to be careful in sharing information that may indirectly lead back to their real identity. The leaders of various major cryptomarkets have been arrested because of OPSEC mistakes, for example, with their personal email accounts. Email addresses registered to their real identity have been used by them to promote a cryptomarket on Web forums, to register servers or in a welcome message to new users (USA v. Ross William Ulbricht, 2013; USA v. Blake Benthall, 2014; USA v. Alexandre Cazes, 2017). Users of illicit online marketplaces must thus make sure they merely use their pseudonyms and do not leave any trace to their 'real-life' identity (Van Hout & Bingham, 2013). This means they should not provide any identifying details to any other member of the community during transactions or private and public forum communications. Cryptomarkets and their users use many mechanisms to enable a working marketplace were participants can trust each other without having to give up on anonymity. Duxbury and Haynie (2017) have even referred to trust as the main stabilising force on cryptomarkets.

1.2.3 Trust mechanisms

Trust has been defined as an attitude of *X* towards the trustworthiness of *Y*. Trustworthiness is context-dependent and trust is thus subjective (O'Hara, 2012). Cybercriminal actors have incentives to remain anonymous to avoid being arrested. Therefore, they do not trust trading partners based on real names. Instead, cybercriminals partly rely on the trustworthiness of a trading partner's pseudonymous online username and the reputation that comes with it (Lusthaus, 2012; Yip, Webber & Shadbolt, 2013; Décary-Hétu & Leppänen, 2013; Martin, 2014; Afroz et al., 2014; Ladegaard, 2017). As members of marketplaces use pseudonyms, unconventional methods are in place to create bonds of trust. A buyer must make sure that a seller is going to send a product instead of simply taking the money and disappearing in realms of anonymity. Therefore, the pseudonym of a trader becomes its identity. According to Lusthaus (2012: p. 80), the pseudonym is the "foundation of their reputation" and the "brand" of the cybercriminal.

Next to relying on the social appearance of a pseudonymous username, cybercriminals have incorporated technical and socio-technical mechanisms in their platforms that can facilitate illicit online trades without having to trust trading partners. Social, technical and socio-technical mechanisms are thus used in pseudonymous cybercriminal environments, such as cryptomarkets, to enable trust. These have been put in place to diminish the reliance on an individual's judgement on the trustworthiness of other actors. The trust mechanisms discussed below can help cybercriminals in determining more objective trustworthiness. In other words, these mechanisms help users in ascertaining that the party they are dealing with has previously fulfilled their part of a transaction and will do so again in the future. Below, in Table 1.3, some examples of these social, technical and socio-technical trust mechanisms are given.

Social	*Technical*	*Socio-technical*
Language	*Tor*	*Voting, reviewing*
Signals	*Cryptocurrencies*	*Lifespan*
Escrow	*PGP*	*Multisignature*

Table 1.3 Examples of trust mechanisms on cryptomarkets

For social and socio-technical trust mechanisms, respectively, the concepts of local and global trust are relevant. Local trust focuses on trusting someone through personal acquaintance, while global trust is basing trust on judgements of a trusted institution (O'Hara, 2004). Local trust will thus be gained between buyers and sellers when the right signals are shown. Examples of these include knowledge of the right 'argot' within the deviant online subculture (Holt, 2010) and ‘lifespan’ in the community (Décary-Hétu & Leppänen, 2013). Argot is the right usage of abbreviations and terms, specifically used within the particular community. In carding communities these focus on financial jargon and “unique slang” (Hutchigns & Holt, p. 603). It is, for example, used to describe the different numbers on the stolen payment card. Lifespan looks at the time users have spent in the community, which can be determined by looking at their number of posts, join date and received recommendations by other users.

Global trust is obtained through technical mechanisms that are controlled by people. Upvotes and downvotes are, for example, a numerical indicator of success or failure within the community. However, members in the community provide these votes and are thus responsible for the success of this mechanism as a measure of trust. This is thus a social-technical trust mechanism, which can contribute to safeguarding the quality of traded goods. Still, there are possibilities to fake such apparent trustworthiness by, for example, writing fake reviews or creating several accounts to upvote another account. These have been respectively referred to as slander and Sybil attacks (Douceur, 2002; Franklin et al., 2007; Yip, Webber & Shadbolt, 2013; Décary-Hétu & Dupont, 2013). These may lead to mistrust and increase the perceived risk by cybercriminals (Hutchings & Holt, 2017). However, these attacks are time-consuming and will thus not always be effective. It will particularly be difficult to attack the trustworthiness of established vendors with many customer reviews and upvotes. Therefore, socio-technical trust mechanisms will often be effective in establishing trustworthiness of cybercriminals.

Multisignature transactions are another example of how technical mechanisms can be controlled by people to establish trust. These are used to prevent scams, which are more likely to happen when buyers ‘finalise early’, i.e. pay for the product before receiving it (Møller, Munksgaard & Demant, 2017; Holt et al., 2015). With multisignature transactions, a third ‘neutral’ party will get involved to provide more security. Instead of directly sending the money from buyer to seller, people have to sign the transaction, depending on the pre-determined cryptographic signature consensus (Brito, Shadab & Castillo, 2014; Horton-Eddison, 2017; Goldfeder et al., 2017). This could, for example, mean that two of three people have to sign before funds get released. If the buyer receives the ordered product, she will sign the transaction and the funds will be released. In case of a dispute, the third party will have to come in and can, for example, sign together with the buyer, to return the money to the buyer's bitcoin address.

Multisignature transactions are an evolution of escrow transactions. These have also been used to ensure that the seller does not take the payment without delivering the product (Yip, Webber & Shadbolt, 2013). When escrow is in place, an intermediary will receive the payment from the buyer and the card details from the seller. With carding, this person will then test the cards and only release the money if they work (Glenny, 2011). However, the third party has to be trusted with escrow transactions, because that person will hold the money and can thus run off with it. In multisignature transaction, the technology has to be trusted and the money will automatically be released after enough signatures by involved parties have been obtained. Escrow is therefore a social trust mechanism, while multisignature transactions are socio-technical.

Social trust mechanisms can be obtained and strengthened over time, but technical trust mechanisms have to be in place when a user starts getting involved on a cryptomarket. A technical measure that is in place by every user of illicit hidden services on the Tor network is, obviously, the Tor browser. This means that users will technically be anonymous, if Tor is secure and does not leak IP-addresses of its users when attacked (Biryukov, Pustogarov and Weinmann, 2013). Cryptocurrencies can also be considered a technical trust mechanism, as their characteristics make it hard to trace back to an individual. Furthermore, users are often recommended to use PGP for sending personal messages in which they discuss transactions. These one-on-one conversations could otherwise give away personal details, for example, when a cryptomarket is seized by law enforcement. Other trust mechanisms that are already, or may be in the future, adopted by cryptomarkets can be classified as social, technical or socio-technical. This distinction is important, as it can help in both understanding how trust is established by cybercriminals and to what extent these bonds of trust can be influenced.

Carding communities have benefited from social-technical growth processes. Groups of heterogeneous actors have come together on IRC platforms, forums and cryptomarkets to achieve similar goals, i.e. optimising the trade in stolen payment details on a global scale while staying anonymous. Over time, the successes and failures of networks have led to other networks adopting similar measures and forming new networks. The social, technical and socio-technical trust mechanisms discussed here are some examples of developments that have been adopted because of socio-technical growth. According to Hendler et al. (2008: p. 67), socio-technical interplay allows for user communities to "construct, share and adapt" to make successful (Web) technologies grow through "trial, use and refinement". However, in the case of members of online communities focusing on the trade of illicit services and goods, such trial and error strategies could lead to serious consequences, i.e. deanonymisation or even incarceration.

1.2.4 Issues for law enforcement in dealing with cryptomarkets

Takedowns of cryptomarkets have been used by law enforcement agencies in an attempt to affect the bonds of trust of cybercriminals, diminish the sale of illicit services and goods, and as a deterrent. Takedowns lead to a lot of media attention. After several takedowns of cryptomarkets law enforcement agencies have spread the message that individuals with illicit intentions are not safe in the perceived anonymous environment of Tor[19] [20]. Such public attention focusing on illicit hidden services can, however, also lead to a rise in people interested in it. Both (prospective) victims and the (prospective) online criminals can be increasingly drawn to the darknet because of hype in the media. The first group's fears may be strengthened by deterrence messages in the media. Law enforcement has an important role in the media's shaping of such 'moral panics', as they have identified the issue and have chosen to amplify their successes through the media (McLaughlin, 2007). McLaughlin has argued that it is tempting for law enforcement agencies to manipulate 'moral panics', as it can lead to increased "resources, empowerment, legitimacy and status" for them (p. 64). This can stand in the way of critical analysis, as reactions are proportional to the panic instead of actual events (McLaughlin, 2014; Young, 2009).

[19] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network
[20] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

Law enforcement's actions can, by doing this, also affect the second group, (prospective) online criminals. Ladegaard (2017) found that media reports that focus on law enforcement's efforts on the takedown of the first Silk Road marketplace did not help in changing users' perceptions of risk or in deterring trade. Instead, increased media exposure led to increased trade. In line with this, both Décary-Hétu and Giommoni (2017) and Soska and Christin (2015) argued that takedowns of hidden services have positive short-term effects, but that marketplaces on Tor are resilient to takedowns by law enforcement in the longer term. There might be short-term effects, such as temporary lower numbers of active vendors, but these recover over time. Yet another risk is that continuous law enforcement interceptions on Tor will lead to users abandoning larger marketplaces and finding alternatives that are more private and even harder to takedown. Such displacement is thus a commonplace issue in addressing cryptomarkets. Taking cryptomarkets down is complicated because of the operational security measures of marketplaces and their users. Moreover, they can be relatively easily set-up again. Therefore, law enforcement agencies, researchers and industry need to think of measures that are not "fire-fighting" measures (Thomas et al., 2015: p. 17). Focus should therefore be broader and look at how technologies change, how fraudsters displace and how their behaviour is non-optimal. This thesis takes such a more holistic approach. Before elaborating further on this approach, related work will be explored to contextualise this thesis.

1.3 Related work

Carding and its related activities have been studied from a wide range of angles since the mid 2000s. In order to place this thesis within that context, the approaches of some influential works are briefly explored below. Thomas and Martin (2006) were one of the first papers to introduce the terminology and divisions of labour involved in carding to academia. Franklin et al. (2007) measured logs collected from an underground market to quantify and categorise participants and products offered by type of goods, type of services, and price. These two papers gave some initial insights into the modus operandi and scope of the illicit trade of carders. Holt and Lampke (2010) further explored online stolen data markets qualitatively to explore what type of products data thieves sell. They found that a variety of stolen information is sold online for profit, but that personal sensitive data and data on credit cards and bank account information were the most prevalent ones.

Soudijn and Zegers (2012) worked together with the Dutch police to access a copy of a carding forum, made in 2008. The researchers got access to public and private message data. They conducted a qualitative textual analysis, from which they created a crime script of the cashing process involved in carding. Soudijn and Zegers consequently divided carding into four phases: preparatory phase, theft phase, money mule phase and cashing phase. They rightfully argued that a good crime script is required before effective situational crime prevention measures can be taken. While providing interesting insights into divisions of labour required in carding, their prevention measures are a bit simplistic. They suggested that forums should be taken out and if that is not possible, market functionalities should be undermined. However, they do not explore how.

Other research did explore in more depth what such functionalities are, for example, based on how participants trust each other in pseudonymous environments. Motoyama et al. (2011) empirically examined both the social networks formed within online underground forums and what products and services are being sold. The authors had access to private messages and focused quantitatively on how trust was established between participants, i.e. number of posts, private messages sent and private messages received before receiving ratings, which indicate trust. Décary-Hétu and Leppänen (2013) explored what signs and signals participants in the online carding community send in order to be successful. They concluded that those that send and decode signals the best get highest rewards. Therefore, they argued that rational cost-benefit behaviour could improve criminal performance. Yip, Webber and Shadbolt (2013) focused on trust on carding forums too, by qualitatively analysing conversations between participants on carding forums. Their research analysed trust from the perspective of transaction cost economics and treated the quality of merchandise and identity of trader as uncertainties and costs to the illicit transactions. The authors suggested that preventing the establishment of initial trust should be a priority for law enforcement agencies.

Holt et al. (2015) analysed user comments on 13 forums on which stolen financial and personal information was traded. They looked at users' comments related to their behavioural responses to risks. They concluded that risks mostly came from within the market and that participants actively engaged in risk-avoiding behaviour by trying to minimise risks and maximising rewards. Holt et al. argued that such behaviour of participants of the illicit market is partly in accordance with rational choice theory. However, they did stress that future research must not just be crime-specific, but also context-specific to fully grasp the factors that may affect risk reduction strategies.

Using the same data as Holt et al. (2015), Hutchings and Holt (2015) utilised a crime script analysis in an attempt to find the steps participants of stolen data markets take to trade. Hutchings and Holt presented their findings according to the universal script of Cornish (1994), which encapsulates 9 scenes: preparation, entry, pre-condition, instrumental pre-condition, instrumental initiation, instrumental actualisation, doing, post-condition and exit. The authors mention security and anonymity as an aspect of preparation, but fail to mention its importance throughout the whole carding process. They analysed fifteen tutorials to provide an overview of the tools being discussed. While not analysing the tools in-depth, the authors provided an interesting superficial and "technology-agnostic" overview (p. 17). Furthermore, they stressed that not all the information relating to security and anonymity presented in the tutorials was correct and that not all marketplaces and actors follow best security practices.

Several others have used crime script analysis to analyse cybercrimes. Some examples include studies on internet-mediated drug trafficking (Lavorgna, 2014), phishing (Lastdrager, 2014), crime in the cloud (Warren et al., 2017), and online trade in counterfeit pharmaceuticals (Lavorgna, 2015). Furthermore, one study specifically used crime script analysis to analyse tutorials, or more specifically: recipes for methamphetamine production posted online (Vidal & Décary-Hétu, 2018). The authors analysed the recipes and methamphetamine production over time with a qualitative content analysis, which they were able to do because the recipes they analysed had a publication date. From this, they showed that legislation led to the adaptation of methamphetamine recipes.

While much previous research has created a broad understanding of cybercrime generally and carding more specifically, it must be noted that many past papers in this field look at these topics from similar perspectives. Particularly rational choice theory, routine activity theory, crime script analysis and situational crime prevention have proven to be popular perspectives to analyse online crimes. Accordingly, Table 1.4 List of cybercrime papers using RCT, RAT, SCP or CSA

presents a non-exhaustive list of papers that have used or have shown support for such theories.

Theory	Authors & year
Rational choice theory	Willison & Lowry, 2018; Hutchings & Clayton, 2017; Møller, Munksgaard & Demant, 2017; Smirnova & Holt, 2017; Holt, Smirnova, Chua & Copes, 2015; Décary-Hétu & Leppänen, 2013
Routine activity theory	Holt et al. 2016; Leukfeldt & Yar, 2016; Reyns & Henson, 2016; Reyns, Henson & Fisher, 2016; Vakhitova et al. 2016; Van Ouytsel et al. 2016; Năsi et al, 2015; Lastdrager, 2014; Leukfeldt, 2014a; Maimon et al., 2013; Kigerl, 2011; Ngo & Paternoster, 2011; Reyns et al., 2011; Bossler & Holt, 2009; Marcum et al., 2009; Holt & Bossler, 2008; Yar, 2005
Situational crime prevention	Hutchings & Holt, 2017; Hutchings, Clayton & Anderson, 2016; Thomas et al., 2015; Hay & Webster, 2014; Leukfeldt, 2014a, 2014b; Soudijn & Zegers, 2012; Willison, 2006
Crime script analysis	Vidal & Decary-Hetu, 2018; Warren et al., 2017; Hutchings & Holt, 2015; Lavorgna, 2015, 2014; Lastdrager, 2014; Soudijn & Zegers, 2012

Table 1.4 List of cybercrime papers using RCT, RAT, SCP or CSA

Many of the above papers have provided novel and valuable insights into cybercrime. Rational choice theory can show the cost-benefit considerations of offenders in their illicit (online) trade. Routine activity theory and crime script analysis have been used to show the most common taken paths in crime commission. Situational crime prevention can consequently look into addressing such common paths[21]. These approaches mostly research the most commonly

[21] In Chapter 2 and Chapter 3 these theories are discussed in more detail

taken recommended paths and accordingly analyse rational decision-making. However, as Holt et al. (2015) have argued as well, information relating to security and anonymity presented in tutorials and on forums used by cybercriminals is not always correct, or even “flooded with misinformation” (p. 96). Furthermore, context may also affect security behaviour (Sawaya et al., 2017). This can lead to failures of following the security practices that are considered best in the online illicit communities. It has been argued previously that online criminals are not strictly rational beings and that (preventative) policy based on such observations could be counterproductive, as they do not address the (local) core of the issue (Cross, 2018) and might simply lead to displacement (Garg & Camp, 2015; Clayton, Moore & Christin; 2015).

Cybercrime research utilising approaches based on rationality have provided many interesting insights. Traditionally, however, criminology has also focused on the decision-making of criminals from more structural and behavioural angles. Other disciplines, such as psychology and behavioural economics, have over the years influenced such criminological research. These lines of research will be explored in **Error! Reference source not found.** to contextualise this thesis. Cognitive biases and contextual factors that affect decision-making are not extensively explored in cybercrime research. Still, they can provide various novel insights into the decision-making of cybercriminals, which can lead to improved countermeasures. Therefore, this thesis will attempt to explore these factors and biases.

1.4 The relevance of contextual factors and cognitive biases

This thesis has attempted to explore how the behaviour of carders can be accurately represented. Utilising crime script analysis, a method originating from rational choice theories, was found to only lead to an optimised representation of decision-making. Such representations are often sufficient to obtain novel insights and are widely used, as described in 1.2. Analysing criminal behaviour through rational choice theories is characterised by the assumption of offenders’ rational decisions, i.e. the decision whether to partake in criminal activity is made by actors who make rational calculations and cost-benefit analyses, allowing for apparent optimal resource allocation (Becker, 1968; Gül, 2009). However, this overlooks that such calculations are made within personal and structural contexts. Therefore, rational choice theories, such as crime script analysis, can sometimes overlook behaviour that does not adhere to the established norms within the researched community. Yet, such possible non-optimal behaviours are often important to explore, particularly in crime research. For example, non-optimal behaviour by carders, and other online offenders, can lead to their possibly deanonymisation and consequent arrest. Therefore, the contextual factors and cognitive biases that can lead to such decisions needed to be explored. This is a contribution of this work to the field.

In working towards this goal, this work has stressed the importance of analysing behavioural biases. In doing so, this work used theories from behavioural economics and psychology to better account for the behaviour of online offenders. This complemented an idealised representation of decision-making, which was established with a crime script analysis of online carding tutorials. This led to a necessary basic understanding of the 'optimal' processes involved in carding. This crime script analysis was then extended upon with CommonKADS models, which looked at what the potential bottlenecks and biases in the usage of recommended tools from the tutorial data were. Furthermore, interviews with experts in the field were conducted to get novel insights into the behaviour of cybercriminals. This further confirmed the importance of offenders' behavioural biases and contextual factors in investigating cybercrime.

The above combination of data and methods was used to both explore online offenders' 'optimal' decision-making and the possible deviations from such norms. This unique approach has led to novel insights into the importance of analysing behavioural biases and contextual factors in cybercrime research. This is the main contribution of this work. The methods used in this work are further explained in Chapter 3. The research questions that were set at the start of this research show how this research has ended up with this combination of methods.

1.5 Research questions

This research has attempted to explore how carders obtain and cash out stolen payment card details. It looked at recommended paths of crime commission in this field, but also at contextual factors and cognitive biases that can influence such 'optimal' decision-making. In doing so, it tried to offer a holistic perspective on carding and contribute to thinking about how countermeasures should be designed. The following research questions were explored in this thesis:

- What steps do carders take to obtain and cash out stolen payment card details?
- To what extent is the mapping of 'optimal' paths useful in addressing carding?
- How can the decision-making of carders be presented more accurately?
- How can the validity of the findings of this work be verified?
- What policy recommendations can be created from mapping the steps carders take to cash out stolen payment card details?

In order to answer these questions, it is described in Chapter 3 what data was analysed, which methods were employed, what ethical issues were considered and what the possible limitations were of the chosen methods.

1.6 Outline of thesis

In this section, an overview of the structure of this thesis is presented. Chapter 1 has introduced the relevance of studying online card fraud. It has also presented a background on carding and on the evolution of certain aspects of cybercrime. It analysed what mechanisms are in place to create bonds of trust in pseudonymous environments on the Web and how this has complicated investigations for law enforcement agencies. Related work was explored and it was discussed how this has influenced the approach in this work. It did this by stressing how this work has acknowledged contextual factors and cognitive biases in its attempt to address a research gap and to explore in a different way how carders operate.

Finally, the research questions and outline of this thesis were presented in this chapter.

Chapter 2 first explored rational choice theory, routine activity theory and situational crime prevention. These theories are the foundation for crime script analysis, a used method in this research, and commonly used in cybercrime research. After this, it looked at how criminological theory has critiqued such theories over the years. It also explored how left realism and the square of crime have been used to provide a holistic approach in the analysis of crime. Furthermore, it looked at how various theories from behavioural economics and psychology can be used to account for the varied reality of criminal decision-making.

Chapter 3 has presented the aim and objectives, dataset and sampling strategies, methods, methodology, ethical considerations, and limitations of this thesis. It has explored in detail how data was collected and how these were analysed. The origins and characteristics of the methods used to analyse data, crime script analysis and CommonKADS, were also presented in detail. Furthermore, the ethical approval processes that were obtained before parts of this research could be started were explained. Finally, possible limitations of crime script analysis, CommonKADS and expert interviews were discussed.

Chapter 4 presented a crime script analysis of carding. It was shown how 25 carding tutorials were analysed and how this led to the creation of the crime script. Situational crime prevention measures derived from the crime script will also be presented. The efficiency of such methods will be debated, which leads into a discussion on the ‘permutation’ concept and into Chapter 5.

Chapter 5 extends on the crime script analysis in Chapter 4 by analysing the organisation and tasks involved in carding through CommonKADS models. Organisation models were presented to show the contextual factors of carding. Task models have shown what tools carders use and what possible bottlenecks they may encounter in these tools in the carding process.

Chapter 6 has presented the first results from expert interviews. First, it has laid out a classification of interviewees. Second, a thematic analysis of expert interviewees’ comments on the behaviour of carders and other cybercriminals was presented. Various comments by interviewees were presented here to exemplify the themes. Third, the interviewees’ comments were analysed in relation to the relevant literature. Finally, possible pitfalls in the behaviour of carders were explored based on the comments by interviewees and the previous findings from Chapter 5.

Chapter 7 also presented a thematic analysis based on the comments of expert interviewees. However, in this chapter the focus lied on the interviewees' comments in relation to the policing of carding and relevant policy measures. The wide range of stakes at play in addressing carding has been explored through the comments of experts from law enforcement agencies, banks and security companies. In an analysis section, these comments were then compared to relevant literature. Finally, it was stressed what elements need to be addressed before countermeasures can be properly designed.

In Chapter 8 the conclusion of this thesis was presented. It explained how this thesis has contributed to a better understanding of the decision-making processes of carders. The contributions per chapter were presented, after which the contribution of the entire thesis was laid out. It also revisited the research questions, discussed possible limitations and explored to what avenues for future work the findings in this research have led. This thesis has shown that cognitive biases and contextual factors need to be taken into account to represent the decision-making of cybercriminals more accurately.

Chapter 2 Rational choice, left realism and cognitive biases

2.1 Background

Much cybercrime research has used perspectives influenced by rational choice theory, routine activity theory, crime script analysis and situational crime prevention. First, this chapter will briefly analyse what these theories entail. Second, a literature review on criminological critiques of such theories will be presented. Consequently, left realism will be presented as a traditionally opposite approach to rational choice theories. It will be shown how left realism has influenced thinking in criminological research and affected the perspectives used in this thesis. Furthermore, theories that have shown irrationality in decision-making will be presented. It will be highlighted how analysing commonly recurring cognitive biases in decision-making can complement research influenced by rational decision-making perspectives. It will then be shown how these cognitive biases are relevant to analyse in the context of the behaviour of cybercriminals.

2.1.1 Rational choice theory

Rational choice theory, in criminology, presupposes that:

> "[...] crime is purposive behaviour to meet the offender's commonplace needs for such things as money, status, sex and excitement, and that meetings these needs involves the making of (sometimes quite rudimentary) decisions and choices, constrained as these are by limits of time and ability and the availability of relevant information."
>
> (Clarke, 1997: p. 9-10)

Rational choice theory in criminology thus looks at the decision-making process of offenders when they commit a crime, which at all times follows cost-benefit calculations and is only limited by time, ability and availability of information (Cornish & Clarke, 1986; Lavorgna, 2013; Hutchings & Clayton, 2016).

Rational choice theory is derived from the economic model of expected utility (Akers, 1990). Expected utility was first proposed by Bernoulli (1738), who referred to it as ‘moral expectation’, a concept to explain differences in individual behaviour when confronted with risky choices. Bernouilli stated that it was originally assumed that if two people encounter similar risks, their desires will also be fulfilled similarly. Economic theories often assume maximising behaviour of subjects and thus have rational choice theory at the basis of analyses (Becker, 1976). Rational choice theory has also been used for the economic analysis of law and is sometimes used by researchers in disciplines as varied as political science, decision theory and history (Ulen, 2000). In criminology, the expected utility model analyses crime under the assumption that criminals become criminally active if they believe their expected utility from crime is larger than the utility obtained from legal activities (Becker, 1968). In other words, if the costs of a crime are higher than the benefits, it will not occur. If the costs are low and the benefits are high, it will occur.

2.1.2 Routine Activity Theory

Routine activity theory (RAT) has been used for describing the circumstances under which offenders engage in "predatory criminal acts", without looking at individual characteristics of offenders (Cohen & Felson, 1979: p. 588). It looks at routine activity patterns of offenders, in which illegal acts are seen as events in space and time. Cohen and Felson’s theory stresses that the commission of crime demands three central elements:

- Motivated offenders
- Suitable targets
- Absence of capable guardians

If suitability of a target is decreased or the amount of capable guardians are increased, crime rates can be diminished, the authors argued. Contrasting with most other criminological theories, RAT does not take offenders’ motivations into account, which according to Clarke (1997: p. 11) "avoids speculation about the source" of deviant behaviour and thus takes the existence of crime as a given, without looking at its cause. From an offender's viewpoint, a targets' suitability is measured by several components: visibility, inertia, value and accessibility, the VIVA acronym (Cohen & Felson, 1979; Yar, 2005). Cohen and Felson concluded, in 1979, that vehicles and electronic appliances are therefore under most risk of theft. A capable guardian does not have to be a law enforcement official or security guard, but can be anyone in the vicinity of a crime who can potentially scare away an offender, Felson and Clarke specified for the Policing and Reducing Crime Unit of the UK Home Office in 1998**.**

Several authors have tested the applicability of routine activity theory to online crime. The importance of the spatio-temporal element in the analysis of crime for RAT has been marked as a limitation of the application of the theory in an online environment (Yar, 2005). While agreeing with Yar (2005) that victims and offenders do not interact physically in 'cyberspace', Holt and Bossler (2008) argued that chances of victimisation may still be increased, if Internet users are more exposed to 'motivated' offenders. They argued that regular use of chatrooms, for example, could lead to increased chances of being harassed. RAT may be more applicable to certain kinds of online crime than others, they argued.

More recently, Leukfeldt and Yar (2016) tested the applicability of RAT on six types of online crime: malware, hacking, identity theft, consumer fraud, stalking, and online threats. They used the VIVA approach to look at targets and at capable guardians to see if targets were attractive for a 'motivated' offender. Their analysis showed that not all parts of RAT are useful in the context of online crimes. Whereas visibility plays a role for all the analysed crimes, accessibility and personal capable guardianship did much less so. The value of a target (victim) and technical capable guardianship showed almost no effects on targets in their study, which is unexpected, as it would be expected that high value targets and a lack of technical capable guardianship would affect victimisation. Williams (2016) used RAT as a framework to show that national cyber security strategies and Internet infrastructure (physical guardianship at a country-level) effects individual guardianship (online identity theft levels). RAT can also be used as a framework to see how an online offender's access to resources can affect motivation, according to Chon and Broadhurst (2014). It thus appears that certain concepts from RAT can be used to analyse online crime, but that its complete successful adoption is hampered by its origin in physical crime, which are difficult to transpose to an online environment.

2.1.3 Situational crime prevention

The theoretical foundation laid out by rational choice theory and routine activity theory was used by Clarke (1983, 1995, 1997) to develop situational crime prevention. Situational crime prevention (SCP) is an approach to crime reduction that, similar to RAT, does not try to change offenders or solve underlying societal issues. Instead, it tries to find measures for specific crimes by altering the design or management of the immediate environment in which the crime gets committed. Its development further depended on the 'action research paradigm', which is the cooperation between researchers and practitioners to identify and solve problems in a recursive manner. Also, opportunity-reducing techniques and a wide body of "evaluated practice including studies of displacement" (Clarke, 1997: p. 6) were part of the original framework for SCP. According to Clarke (1997: p. 26), situational crime prevention methods "usually ameliorate, not eliminate a problem". Such displacement is a common result of SCP measures, as the causes of crime are not addressed and altered (Hesseling, 1994).

As a theoretical underpinning of SCP, Clarke describes the opportunity structure of crime, which consists of three components: targets, victims and crime facilitators. The physical environment, lifestyle and routine activities of a population determine the supply of targets, according to Clarke (1997). This, in turn, is determined by the socio-economic situation of society, which also partly determines the number of potential offenders and their motivations, he argued. However, while acknowledging the socio-economic causes of crime, SCP still chooses to ignore them in its analyses, instead focusing on measures that can lead to a reduction in opportunity for crime. Initially, four classes of opportunity reducing techniques were identified: *increasing perceived effort*, *increasing perceived risks*, *reducing anticipated rewards,* and *removing excuses* (Clarke, 1997). Per class, there are four types of opportunity-reducing techniques. Clarke argued that such opportunity-reducing techniques can diminish the chances for crime and make it less rewarding and excusable.

After Wortley (2001), who stressed that situations itself can be a motivation to commit a crime, critiqued Clarke's opportunity-reducing techniques, Cornish and Clarke (2003) altered several techniques and added some, of which the *reduce provocations* class was new to the situational prevention opportunity reduction techniques. The newer approach thus allows for the acknowledgement of "moral scruples" of an offender (Cornish & Clarke, 2003: p. 80), which may or may not be altered by situational cues. However, Cornish and Clarke argue that such acknowledgements will only affect motivations in the longer term and will not immediately lead to crime reduction. They stress that SCP is easier applicable when a rational choice approach is assumed, as it then purely focuses on how crimes are committed. They ascribe this to the "necessary simplifications of good enough" policy-oriented theories for practice (p. 86).

Several studies have already applied situational crime prevention to find possible intervention points, after finding common paths taken by criminal decision makers with crime script analysis, as will be shown below.

2.1.4 Crime script analysis

Crime script analysis (CSA) was created by Cornish (1994). The origins of crime script analysis lie partly within the area of rational choice theory. Cornish (1994) specifically described the unfolding of criminal events as an aspect of rational choice theory, which was developed further with the conception of crime script analysis. Parts of CSA are, however, also partly based on RAT and SCP. Moreover, the script approach is based on the work of Schank and Abelson (1977), who argued that human knowledge of procedures could be presented in scripts. Cornish (p. 175) therefore described crime script analysis as a way of "highlighting the procedural aspects of crimes." It outlined all the actions that have to be performed in preparation, execution and completion of a certain offence. It can help to understand crime types, deconstruct a (complex) crime into its integral parts and consequently contribute to the development of crime prevention programs (Brayley, Cockbain & Laycock 2011; Hutchings & Holt, 2015). However, the original main goal of crime scripting is situational crime prevention.

Cornish (1994) suggested that a crime script approach can enhance SCP, as it points to more possible intervention points and, in this way, can complement crime reduction policies. However, recent research using CSA has not necessarily had SCP as its goal. Scripting has, for example, also been used to find criminal opportunities and identify behavioural patterns, as shown by Lavorgna (2014). Crime scripts are written from an offender's perspective and focus on casts, actions, props and locations. Casts are the people (users in an online context) and victims an offender interacts with in the criminal process. Actions specifically describe the steps involved in the offence. Props are the facilitators that make the offence possible. Location describes where specific parts of the preparation, execution and aftermath of an offence occur (Cornish 1994; Borrion, 2013). To apply crime script analysis to an online environment, the differences between traditional, i.e. physical, and online crime have to be taken into account. The dynamic nature of online environments leads to the fact that script analysis is more limited in its capacity to identify simple preventive measures than with physical criminal activities (Lavorgna, 2013).

Cornish (1994) initially focused on street crimes, such as robbery, graffiti tagging and auto theft. However, over the years, crime scripting has been used for a wide range of more international and complex crimes. Some examples of these include counterfeit alcohol trafficking (Lord et al., 2017), money laundering (Gilmour, 2014), child sex trafficking (Brayley, Cockbain & Laycock, 2011), and online drug trafficking (Lavorgna, 2014). The focus of this work, carding, is also a more international and complex crime than the initial crimes that were analysed with crime script analysis. According to Cornish (1994: p. 175), crime scripts emphasise "the form of crime as a dynamic, sequential, contingent, improvised activity, and the content of specific crimes, considered as activities with particular requirements in terms of actions, casts, props, and spatio-temporal locations." This can be largely applied to the types of offences committed via online criminal forums or marketplaces. However, as online criminal forums and marketplaces have an international and anonymous nature, spatio-temporal locations will not be as relevant as in crime scripts for traditional street crimes. Therefore, the focus in this research was more on casts, actions and props. An in-depth analysis and modelling of these elements could then, in theory, contribute to exposing weaknesses in carders' operational security and address these with situational crime prevention measures.

2.2 Critiques of rational choice models

The underlying assumption of rational choice models is that behaviour can be explained in economic terms of benefit and costs. According to Clarke (1997: p. 9), rational choice theory has departed from such expected utility theories "to give greater weight to non-instrumental motives for crime and the "limited" or "bounded" nature of the rational processes involved." Consequently, rational choice theory assumes that crime is purposive behaviour, only limited by time, ability and availability of information.

Situational crime prevention tries to modify the settings in which crimes occur and does not look at individual motivations for crime commission and societal issues. However, it is often impossible to change the settings in which a crime occurs or such adjustments will simply lead to displacement. This is especially the case in the online realm as online criminals are using legitimate tools to stay anonymous, such as virtual private networks (VPN), encryption and Tor. Also, for example, tools used for (online) money laundering are also used for legitimate purposes, such as cryptocurrencies, vouchers and a wide range of legitimate online payment services. Altering these tools, which would be a SCP solution, could impact the privacy of citizens and negatively affect business processes. However, it must be acknowledged that there are ongoing debates on such issues, for example about encryption and Tor (Moore & Rid, 2016; Guitton, 2013), in which the privacy and security benefits for citizens on the one hand and possibilities for abuse by malicious actors on the other are often used in favour and against widespread use of such technologies.

Rational choice models assume paths to perfect anonymity if the right information is available. This disregards the omnipresence of cognitive biases in decision makers. Carders make mistakes, which can be exploited by parties trying to lead back to their real identity. They might even make ‘mistakes’ willingly to save time or because of their misunderstanding of information. Being overly confident in risk judgements could lead one to purposively skip steps in recommended crime commission processes, for example in tutorials, and come up with their own methods to cash-out. Moreover, tutorials can also contain non-optimal advice, especially as optimal paths may not exist or are temporary and location-dependent.

There are clear advantages to assuming the rationality of actors in modelling efforts. If all actors in a model are rational, solutions can be uniformly designed. Therefore, rational models can seemingly create more impressive results than other theories. Assuming full rationality amongst actors, however, does not account for the varied reality of human actions. According to Kahneman (2003: p. 706), rational models assume that agents make choices in a “comprehensively inclusive context”, in which relevant information is available and being used by the actor and decisions can thus be made with present and distant risks and opportunities in mind. Crime script analysis and situational crime prevention use a ‘bounded’ rationality perspective, which assumes that offenders purposively commit crimes to meet their needs, but are bounded by time, ability and the information that is available to them (Clarke, 1997). While this is an improvement of a fully rational choice approach, it should be acknowledged that actors are also ‘bounded’ because of many other behavioural biases. This may seem trivial, but assuming rationality amongst actors could, for example, lead to oversimplification of policy design (Garoupa, 2003). Therefore, wider ranges of influences that affect human behaviour also need to be studied. This has been acknowledged in various strands of criminology for decades.

2.3 From positivism to left realism

Rational choice theories assuming utility maximisation may ignore factors that influence human decision-making. These include, but are not limited to, social structures (Merton, 1938; Holt & Lampke, 2010), values and moral judgements (Akers, 1990), reference groups (Runciman, 1966; Webber, 2007b), subcultures (Cohen, 1956; Holt, 2007) and many types of behavioural tendencies that will be discussed later in this chapter. Still, rational choice theory has enjoyed great popularity in sociological and criminological theory. According to Hayward and Young (2004), and many other criminologists (Walters, 2003; Matthews, 2014; Tierney, 2010; Garland, 2001), rational choice theory and positivism have dominated the field. Positivism is an approach “that sees science as necessarily objective and value free”, which looks for general principles “on which to base predictive laws” (Halford, Pope & Carr, 2010: p. 3). Economic rationalism and managerialist philosophies in academia are responsible for the dominance of the two strands, according to Walters (2003). He states that research has been directed to projects that are in search of answers to crime causation and improving “apparatus of crime control” (p. 23).

What can be missing from such works are narratives that link factors to outcomes, the Weberian “*verstehen* of human meaning”, to explain that correlation is not the same as causality (Young 2004: p. 13). Crimes are not always committed by a calculated rational object, which is assumed in rational choice theories and positivistic approaches. Instead, many crimes, especially petty crimes, are caused by boredom, or “an existential disjunction between expectation and experience” (Ferrell, 2004). The search for excitement, i.e. ‘getting the buzz’ (Webber, 2007a) or the search for an ‘adrenalin rush’ (Ferrell, 2004), is thus often at the foundation of such offences. Cultural criminology addresses such issues by viewing “crime and its control in the context of culture: that is, viewing both crime and the agencies of control as cultural products—as creative constructs” (Hayward & Young, 2004: p. 259). It uses ethnographic methods to explore individual subjects and stands in contrast to rational choice theory and positivism, which according to some authors can exclude ambiguity and human error from its research (Ferrell, 2004; Hayward, 2016). Cultural criminology does focus on such factors, but within the limits of localities and groups. This makes drawing generalised conclusions or meaningful policy from its analyses difficult (Matthews, 2014; Webber, 2007b). Therefore, this work uses another criminological perspective, left realism, to inform its analyses.

Left realism emerged in the 1980s as a reaction to the overtly punishment oriented approaches of neo-liberal governments, such as Margaret Thatcher’s in the UK and Ronald Reagan’s in the USA (Young, 1997). Such governments proposed ‘tough on crime’ approaches to deal with offenders (Matthews, 2009). Left realism stands in opposition to rational choice theory and other “administrative and scientific criminological knowledges that have traditionally appealed to governments” (Walters, 2003: p. 16). Young (1997) argued that left realism is not like rational choice theories and thus not:

> “a cosmetic criminology of an establishment sort which views crime as a blemish which, with suitable treatment, can be removed from the body of society which is, in itself, otherwise healthy and in little need of reconstruction.” (p. 472)

Instead, left realism tries to bring all aspects of the process of crime together in its analysis. It argues against ideas that came up in the 1970s in both administrative criminology on the one hand, which prescribed pragmatic situational crime prevention measures and heightened levels of security, and Marxist perspectives, which were too idealistic, on the other (Hayward & Young, 2004; Lea, 2015; McLaughlin, 2007). Such Marxist perspectives saw criminality by marginalised groups as a form of rebellion in reaction to a combination of criminalisation by state elites and moral panics in the media with no basis in reality. These perspectives made it appear as if crimes were only committed by the state and capitalist class on the one hand against the working class and marginalised groups on the other (Young, 1987; Lea, 2015, 2016; Webber, 2007a). However, such Marxist approaches have been classified as idealistic, as they overlook the impacts of crime as experienced by victims and the fact that crimes are often committed by the poor (Winlow & Hall, 2016; Lea, 2015). Marxist approaches in criminology thus limit oneself to the dialectic between the bourgeoisie and proletariat. Left realism, instead, uses relative deprivation, an outcome of social comparison processes, as a concept to explain causes of crime, which implies that crime can occur in all parts of society, as long as one person feels relatively deprived compared to the other (Young, 1997; Webber, 2007b, 2010; Runcimann, 1966). This is a more comprehensive and modern perspective to explain underlying causes of crime.

The social context in which a crime is committed is of importance to left realism. Hereby, it stands in contrast to administrative and rational choice criminology, which looks at individuals rather than at their (societal) contexts. However, the two approaches can complement each other, as rational choice theories can be used to explore offender's common ways of executing crimes, while left realism can be used to understand the context in which crimes occur and help thinking about effective countermeasures that do not simply lead to displacement. Left realism employs 'a square of crime' as a framework for the analysis of the context of a crime (Young, 1997; Lea, 2016). It involves the interaction between state agencies (law enforcement, prosecution services etc.), the public, the victim and the offender. It acknowledges that the social context of crime is determined by the social interactions of these four elements and their place in the wider social structure. Crimes are not standalone acts. They are the outcomes of interactions and processes, rooted in the underlying structures of society (Young, 1997; Matthews, 2014).

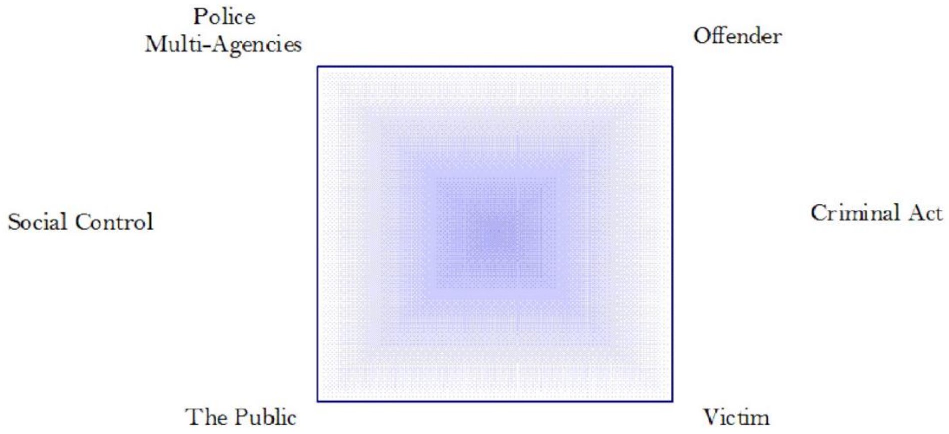


Figure 2.1 Square of crime[22]

It has been argued that not many analyses have deployed all four elements of the square of crime (Young, 1987; Matthews, 2009). Approaches that do not adopt all the dimensions of the square into their approach can be partial and one-sided.

[22] Donnermeyer & DeKesedery (2008)

The square of crime acknowledges the importance of the intertwining of structure and agency for the analysis of crime. In principle, the square of crime can be applied to all types of crimes. However, the square of crime is a representation of the criminalisation process and is only effective when all the elements are interlinked. Or, as Lea (2016: p. 63) has put it:

> “it works effectively where the offender is weak; the definition of crime is consensual; where the community recognises the victim, condemns the offender and supports the criminal justice agencies; and where the latter support the victim and prosecute the offender”

Insights from the square of crime originally focused on local democracy and were dependent on the flow of information between the community and the police, the trust of the community in the police and the democratic accountability of the police (Lea, 2016). International forms of (online) crime will thus be more difficult to analyse, because of the complex nature of these crimes and the interactions between the numerous participants that have to be looked at in such an international setting. Still, the square of crime can be used to look at how types of crime can be explained by social causes and how the interplay between the various international participants in the square of crime affect each other. Therefore, it is a starting point for critical analysis of crime (Lea, 2016). While this thesis mainly focuses on offenders, carders, the other corners of the square of crime are also touched upon at various stages. The victim and the public are more implicitly present in this work, as this work can contribute to measures that reduce the number of victims and consequently improve the public’s perception of law enforcement and card issuers. The national and international cooperation of banks, card issuers and law enforcement agencies against carding are, however, explicitly discussed in Chapter 7.

In the Conclusions and future work section, the square of crime is again used to propose some possible methods for interception and prevention for carding in its international context. In this manner, left realism is thus used to critically analyse carding and to complement administrative and rational choice approaches. First, however, possible cognitive biases in decision-making processes of (online) offenders will be explored. This will point to commonly recurring cognitive biases, which can also complement administrative and rational choice models as these often overlook such mistakes.

2.4 Theories explaining 'irrationality'

2.4.1 Prospect theory

Rational decision-making by agents is assumed in almost all economic theories to explain behaviour (Kahneman, Knetsch & Thaler, 1991). Rational choice models have also been influential in numerous other fields, such as law (Ulen, 2000) and criminology (Becker, 1968). Over time, however, scholars started to see the need for empirical theories that describe actual behaviour, in contrast to an idealised representation of decision-making, such as rational choice theory (Guthrie, 2002). One of the most influential theories trying to deliver such perspectives on decision-making is prospect theory. Kahneman and Tversky (1979) created prospect theory as a critique of expected utility theory and rational choice theory, by modelling decision-making under risk. Prospect theory has shown that people perceive outcomes as gains and losses, not as a final state of wealth. Such gains and losses are held against a neutral reference point, which mainly depends on the current asset position of the decision maker. It also depends on the formulation, or framing, of prospects whether outcomes are seen as gains or losses. Kahneman and Tversky found that responses to losses are generally more extreme than responses to gains. People are thus loss averse. Consequently, losses will have a greater negative psychological impact on an actor than gains have a positive impact. People will thus be more willing to risk more to avoid losses than they would to make gains, as losses can cause greater psychological harms (Jervis, 2004). This is not in agreement with expected utility theory, in which actors would feel and act the same if they had the same amount of wealth, no matter whether they had just won or lost something (Bernoulli, 1738/1954; Kahneman, 2011).

The effect of an actor's reference point in prospect theory can be compared to relative deprivation theory. Relative deprivation is a sense of deprivation, which implies that a person feels deprived. However, this sense of deprivation cannot always be shown statistically, but is merely a personal feeling of deprivation and can thus be found in both the rich and the poor (Runciman, 1966; Webber, 2007b). In prospect theory, similarly, losses and gains can only be explained when looking at an individual's reference point. Reference points are important for decision-making, but also for forming impressions and judgments. A context in which an individual is situated can partly determine the reference point of that individual (Guthrie, 2002). Also, the skills of the carder, expected gains and subjective likelihood of being caught will affect the reference point. Again, the notion of *verstehen* is thus important in understanding human actions. It has been suggested that the effect of context will be even stronger in real-life situations where probabilities and outcomes are not known with absolute certainty, such as in lab settings (Hershey & Schoemaker, 1980). Expected utility theory ignores such context and its effects on preferences (Lattimore & Witte, 1986).

In a simple hypothetical rational choice model, for carders on cryptomarkets for risk-seeking decision-maker *A* and risk-avoiding decision-maker *B* can, for example, be explained by the below, where *O* stands for *operational security*, *G* for *financial gains* and *R* for *imprisonment risk*:

$A = (O\downarrow, G\uparrow, R\uparrow)$

$B = (O\uparrow, G\downarrow, R\downarrow)$

This may then, for example, be explained by this probability:

$C = (0.25, 5000, 0.30)$

$D = (0.50, 2500, 0.10)$

C is the risk-seeking decision-maker who only uses 25% of the available operational security mechanisms, which leads to expected gains of 5000 and a 30% imprisonment risk. *D* is the risk-avoiding decision-maker, who uses 50% of available operational security measures, which leads to half of the gains of *C*, but also *D*'s chance of staying out of prison would, in this hypothetical case, be three times as small.

Whereas such hypothetical rational choice models can be useful as an indicator of how most users are supposed to act, they may overlook context, i.e. the factors that influence decision-making. These are particularly interesting for analysing the behaviour of online criminals, as they can show possible weaknesses in their operational security. Using more tools may not necessarily mean having lower imprisonment risk or less financial gains, which is assumed in the above hypothetical rational choice model. This shows that there is an incentive to explore factors that lead to non-rational decision-making.

All carders will, it can be assumed, try to follow the reference point to stay out of hands of law enforcement. However, users will have different understandings on how to achieve this, depending on their context and cognitive biases. Therefore, the above probabilities are not accurate. Decisions in which way to cash-out a card can depend on the current popularity of a method on forums, on previous personal success or failure in trying a specific method, on how much a user values security over usability and so on. For example, when a user has read about other users getting arrested as a consequence of using a certain anonymisation tool or cashing-out method, the user will be less likely to adopt such a method, because it has the potential to lead to a loss that clashes with the reference point, which in this case is not getting arrested. However, another user might not have read the forum posts, which can thus lead to different decisions. This will lead to the fact that some users may believe that they can stay out of hands of law enforcement by simply using Tor and cryptocurrencies, while others may believe that it is also necessary to use VPNs, MAC address changers, various anonymous credit cards, drop addresses and so on. Reference points thus differ, based on previous experiences and backgrounds of users.

The fact that reference points can be changed over time and that they may depend on vague formulations can offer opportunities to law enforcement in addressing online crime. In optimising their security measures, users will make different choices. Varying degrees of security behaviour has, for example, been shown across different cultures (Sawaya et al., 2017). The habitus of people across cultures can thus determine their security behaviour. While tutorials exist to provide users with the perceived safest ways of doing transactions on underground forums, these tutorials do, however, not provide users with one ultimate way of executing their illicit transactions, as security measures will always be updated depending on recent arrests, technological advances and disagreement within the community. Indeed, large parts of the processes which users of underground forums go through will be largely improvised based on individual reference points. For example, if a certain VPN-provider cooperated with law enforcement to arrest an online criminal, the users that will find out about this information will alter their reference points concerning VPN usage and be more cautious in which one they use. Prospect theory thus shows that people are not always rational in their decision-making, as they are more loss averse than they are positive towards gains and always act according to a temporal reference point. This means that when various options are presented to a group of people, they will not all act in the same 'rational' way.

2.4.2 Status quo

Status quo bias is also a behavioural tendency that affects an individual's reference point and should be taken into account when considering the varied reality of decision-making. Samuelson and Zeckhauser (1988) found in their experiments on decision-making, on health insurance plans and division of retirement contributions, that individuals show status quo bias in simple hypothetical decision tasks. Convenience, habit, inertia, policy (by a company or government), custom, fear, innate conservatism and simple rationalisation are their explanations for a status quo bias. Lack of attention has also been identified as a cause of status quo bias, which leads to the fact that default options can be used to 'nudge' people in a certain direction (Thaler and Sunstein, 2008). Thaler and Sunstein give the example that when a magazine subscription automatically renews, rates of renewal will be much higher. While the reader may not want to renew, making a phone call to actively cancel a subscription may be seen as too much hassle. The status quo is thus in many cases likely to prevail.

Again, it is reasonable to assume that in the complex real world, i.e. outside of experimental settings, status quo bias will be even more visible. Samuelson and Zeckhauser have argued that in some cases, unlike experimental settings, an individual might not even be aware of the fact that there are other options, which makes a status quo prevail. In continuously changing cybercriminal environments, a status quo position in decision-making can be a risky one. New vulnerabilities in tools or markets will come to light and will be exploited by law enforcement agencies to deanonymise users of cryptomarkets. Old operational security measures, that will have kept users safe for long periods of time, may become inadequate and consequently the risk of arrest can increase. Users who suffer from status quo bias may be at risk of deanonymisation, but it does not necessarily mean that it will have consequences. Law enforcement agencies have inadequate resources to track every online criminal and will have to make choices of who to persecute due to restrictions on budget, 'manpower' and capabilities. However, status quo bias will make it easier for law enforcement to target users, as mistakes they have seen before will most likely be repeated.

2.4.3 Overconfidence

It has been suggested, even by some of crime script analysis' early supporters (Ekblom and Gill, 2016), that offenders' stereotyped responses, or scripts, are not always adequate to successfully achieve goals and that a failure to improvise may lead to errors. While status quo biases are present, the status quo is most likely not an optimal, faultless path. Non-optimal decision-making can occur for various reasons: failures to adapt to technological innovation, inattentiveness and laziness are some of the reasons. However, it must be noted, that optimal paths will be continuously shifting and might not even exist, as technological developments are occurring at a rapid pace.

Still, trying to stay up-to-date of essential steps in security is hard, time-consuming and, consequently, can be seen as an obstacle that stands in the way of a primary task (Bada, Sasse & Nurse, 2015). It could also be argued that criminals underestimate the chances of being arrested and as a result take their security steps less serious. Sunstein (1998) refers to such behaviour, the idea that risks will happen to others but not oneself, as systematic overconfidence in risk judgements. People think that low-probability risks are more likely to materialise for others than for themselves. In prospect theory this is explained by the finding that people are limited to comprehend and evaluate extreme probabilities (Kahneman & Tversky, 1979). Unlikely events are thus overweighed or ignored. Sunstein (1998) argues that while people may believe that low-probability events are more likely to occur than their probability, they do not believe this for themselves. If applied to cryptomarkets, many users will thus overestimate the chances of arrest, but may not adapt their security behaviour accordingly. Another characteristic of criminal behaviour that contributes to this is the lack of oversight when it comes to cost and benefits. Benefits are often immediate, while costs (such as incarceration) may come much later (Jolls, Sunstein & Thaler, 1998). The costs are thus incommensurable to financial gains and impossible to calculate.

2.4.4 Workarounds and non-compliance

Literature on workarounds and non-compliance provides more indications on the fact that actors often find their ways around paths that are deemed optimal. Kirlappos, Parkin and Sasse (2014) asked employees of a large multinational organisation about their ‘shadow’ security behaviours, i.e. the behaviour when employees do not follow the policy of the organisation and devise their own solutions for security problems. Shadow security behaviour shows that compliance is not binary: there is more than following or not following up security measures. Employees can also come up with their own measures. An example on an organisational level is that a password policy requires employees to have very strong and different passwords for various applications, which could lead to an excessive cognitive load (Kirlappos, Parkin and Sasse, 2014). Employees may start writing down passwords, which can be against the organisation’s policy, but will still help the employees to comply. While the research in these areas is often focused on organisational settings, it can inform research on online offender’s decision-making as it can be argued that cryptomarkets and other illicit marketplaces and forums are the work environment of offenders. In such criminal ‘workplaces’, forum rules, tutorials and security advice in forum discussions can be seen as company policy. Members of these forums and marketplaces will have similar reasons to find workarounds or to be non-compliant as employees of legitimate organisations.

Lack of awareness about security risks or renewed company security policies, disruption of primary tasks, and inability to comply technically, are reasons for employees within organisations to adopt non-compliant behaviour (Kirlappos, Beautemont & Sasse, 2013; Kirlappos, Parkin and Sasse, 2014). Kirlappos, Parkin and Sasse (2014) argue that, when it comes to lack of awareness about security risks, employees underestimate risk mitigation that can be achieved by complying with their company's security policies. This is why non-compliance is sometimes seen as an easier and more attractive option. Furthermore, complying with security policies is not the primary task of employees and can be seen as a burden that prevents them from doing their actual tasks (Bada, Sasse & Nurse, 2015). Finally, technical non-compliance can occur if the employee does not understand the measures that have to be taken, does not have access to them or does not manage to install required software updates. Similar forms of non-compliance may also occur in online offenders. Online criminals may not be aware of new vulnerabilities in tools or may, for example, not have read updates provided by the marketplaces' leadership. They might also believe that taking certain security steps are not necessary, because of status quo bias for example, as they believe it will not put their anonymity in danger. Also, they might see security measures as a distraction from their primary tasks of making illicit profits. Finally, they might not understand how to use tools and techniques that will keep them anonymous.

2.4.5 Socio-technical co-constitution of knowledge

It has been argued that rationality in decision-making will occur because of an evolutionary argument (Ekblom & Gill, 2016). In such arguments it is assumed that people will learn from irrational decisions and become more rational. This may certainly work in lab settings, where decisions have immediate consequences and feedback is accurately provided. However, such feedback on situational conditions and on a fitting response is often lacking (Tversky & Kahneman, 1986). Especially in online environments, where digital traces are easily left behind, slowly building up more rational decision-making skills will be risky for offenders. There are well-known examples in which online criminals have been arrested because of traces they left behind in the early stages of their online 'criminal career', such as the creator of the first Silk Road marketplace (USA v.

Ross William Ulbricht, 2013). Such mistakes may inform the decision-making of some members of future generations of online criminals. New mistakes will still come to light and offenders will still be arrested. However, the manner in which decision-making on socio-technical structures, such as online criminal forums and marketplaces, is informed by the co-constitution of knowledge, is worthy of further exploration.

Knowledge on online criminal decision-making is often co-constituted through a mix of discussions on forums, top-down messages from a marketplace's leadership and through free or paid-for tutorials. In these supposedly optimal paths in online crime commission are discussed. While this has importance in the evolution of the decision-making process, individual contexts, experience and reference groups also contribute to shaping the decision-making process. For example, if an offender who originally was involved in street crimes gets involved in the online drug trade, he or she might not be used to new technologies and could struggle to adopt an effective path to anonymity. Such an individual is probably more likely to make technical mistakes than a technically-educated university student who similarly decided to start dealing drugs on cryptomarkets. However, the 'traditional' offender may be better in the physical aspect of the illicit trade, such as cashing, laundering and using middlemen. Again, the behaviour of offenders will thus depend on their contextual reference points.

Acknowledgement of various reference groups, on which reference points can be based, explains that (online) offenders are not "uniformly deviant" (Webber, 2010: p. 94). For the former street criminals, using a VPN might be seen as sufficient for online security. They could, for example, be more aware of making money streams appear legitimate and depend on their previously established offline networks for doing so. A computer-savvy technically-educated student, on the other hand, might use a wide variety of tools to stay anonymous, but might go to an ATM or talk over the phone about committed crimes and can consequently be tapped and apprehended by law enforcement. Such contextualised decision-making can be explained by two cognitive systems.

2.4.6 Fast and slow thinking

Non-rational decision-making under uncertainty, such as shown in prospect theory and other theories, can be better expressed by a model of human cognition as two systems. These represent the distinction between intuition and reasoning. The systems are often referred to as System 1 and System 2, but are also respectively referred to as fast and slow thinking (Kahneman, 2011). System 1 is characterised by automatic, quick, largely unconscious, associative and effortless processes. System 2 is characterised by slower, more analytical, effortful and deliberately controlled mental processes (Kahneman, 2003). Furthermore, the operations of System 1 are influenced by contextual, personal and social experiences, whereas System 2 is more rule-based and "encompasses the processes of analytic intelligence", i.e. more based on 'rational' thought processes (Stanovich & West, 2000: p. 658). Thinking about how to cash-out stolen payment card details step-by-step can thus be attributed to slow thinking. However, steps within these processes are intuitive. These parts can be ascribed to fast thinking and might not involve optimal decisions, as such thinking can lead to systematic errors in one's thinking which can give users too much confidence in held beliefs (Kahneman, 2011; Sunstein, 1998).

Methods based on rational choice theory, such as crime script analysis, will take more of a System 2 perspective, as they assume that actors have extensively deliberated over their actions and decisions in the criminal process. The parts of the decision-making process where actors have operated from System 1, in a more associative and context-based manner, is more likely to lead to mistakes. On the one hand, System 2 checks the intuitive judgements by System 1, whether they are safe and/or effective. It accepts or overrides them, but sometimes System 2 can lazily accept intuitive judgements, as one of its characteristics is "laziness, a reluctance to invest more than is strictly necessary" (Kahneman, 2011: p. 31). Such laziness can potentially be used by law enforcement. When users of underground forums only do what is strictly necessary, they might easily make mistakes in their security measures. This is the case, as their reference points might give them a wrong definition of what is strictly necessary. However, on the other hand, the more "complex cognitive operations" eventually move from System 2 to System 1, once they are learnt (Kahneman & Frederick, 2002: p. 3). This may lead to less mistakes being made when time is spent learning the ‘tricks of the trade’. Still, fast and slow thinking can help in explaining why common deviations from the criminal norm occur.

2.5 Discussion

In this chapter various behavioural theories have been presented to show that there are valuable theories that can complement the analysis of (online) crime. Next to purely rational choice theories, bounded rationality perspectives also do not always fully account for the reality of decision-making, as has been shown in this chapter. This is the case, as users are limited by more factors than time, availability and skills, as Clarke (1997) has suggested. Status quo bias, loss aversion, laziness, workarounds and overconfidence are examples of cognitive biases that can also stand in the way of (bounded) rational behaviour. Contingencies that lead to pragmatic decisions will occur in criminal decision-making, off- and online. The discussed cognitive biases are some examples of factors that contribute to the ways in which crimes are executed. By taking these into account, rational choice models can be complemented and inform future research that looks into explaining and addressing online crime.

Chapter 3 Methodology

This chapter presents the aim and objectives, types of data, methods, methodology, ethical approval processes and possible limitations of the methods in this work.

3.1 Aim and objectives

The aim of this thesis was to study the decision-making of carders and to show how this can be influenced by cognitive biases and contextual factors. In doing so, it has tried to provide a perspective that analyses both rational and non-rational decision-making. Throughout this thesis it will be shown that decision-making is not only affected by time, ability and available information, as has been argued in (bounded) rational choice theories. Cybercrime research has often utilised such perspectives, as has been shown in 1.3. While such factors affect the decision-making of online criminals, many other contextual factors and cognitive biases also determine what steps are taken. This thesis has therefore sought to complement previous studies by presenting the factors that may influence (online) criminal decision-making in more detail. This thesis has thus analysed some of the contextual factors and cognitive biases that such previous research has overlooked.

The first objective of this thesis was to create a representation of the 'optimal' decision-making of carders. A second objective was then to discover how and at what stages deviations from this optimal path, i.e. possible non-optimal behaviour, could occur. Analysing what this non-optimal behaviour entailed was a part of this. A third objective was to obtain the perspectives of experts on the behaviour of carders and to see to what extent this influenced their policing of cybercrime.

This work has attempted to answer these objectives in several ways. First, by creating a crime script analysis of carding tutorials, which describe security steps and cashing out methods, recommend paths of crime commission could be mapped. Second, possible non-optimal behaviour was mapped by further exploring the organisation and tasks involved in carding in more depth. The CommonKADS method was used for this analysis. Third, experts from law enforcement agencies, government, banks and the security industry were interviewed to obtain their insights into (online) criminal decision-making and cybercrime policing. Such perspectives are not available through other types of public data and are therefore unique. This unique combination of data and methods, described throughout this chapter, has led to new insights into the decision-making of carders. Both the new insights in the way cybercrime can be studied and the results from the studies in this work are the main contributions of this work.

3.2 Tutorial data

Tutorials posted on cryptomarkets were one of the main data sources for this research. These are a novel source of data, as they have rarely been used for scholarly purposes before. The forum of the cryptomarket where the analysed set of tutorials was found on was taken offline during this research. This also contributed to the novelty of this research, as it is currently difficult to obtain this dataset, unless crawling efforts were set-up before the takedown of the cryptomarket. Tutorials were used to get an idealised insight into the decision-making process of carders. Below, it is explained why and how tutorials were selected as a data source.

3.2.1 Carding tutorials

Forums and online marketplaces focusing on illicit activities often exhibit learning structures that focus on providing members with the perceived safest methods to engage in illicit transactions. The steps that have to be taken by members are often similar and are presented in tutorials. These can both focus on specialised knowledge or on more general knowledge (Yip, Webber & Shadbolt, 2013). While some tutorials are offered for free, the majority is offered for a price. Specialist tutorials from which potentially large amounts of money can be obtained are sometimes offered for several thousands of dollars, and can even come with personal guidance and a training process. Such tutorials will first be tested by a high-up, verified member of the community, to check whether the method is as effective as advertised. Once approved, it will be possible for ‘normal’ members of the community to then purchase the method.

Beginner tutorials are offered for much lower prices, generally less than a hundred dollars, and focus on new members in the community that are inexperienced. Therefore, they focus on basic steps one has to take to engage in a successful transaction and how to stay anonymous in the process. Encryption techniques and proxy services, such as PGP and SOCKS5 will, for example, be explained in them, as these can make it much harder for law enforcement to lead back to the IP addresses of users. Tutorials sometimes get leaked in the community to provide new members with free information on how to become successful members. This provides researchers with an opportunity to get a better understanding of the various steps members of criminal communities are advised to follow. Several cybercrime researchers have used online tutorials as a part of their dataset (for example: Vidal & Décary-Hétu, 2018; Hutchings & Holt, 2015; Lavorgna, 2014). As the steps that users of criminal marketplaces are advised to take are thus often similar, crime script analysis is a method that can seemingly grasp the advised criminal transaction processes, as will be shown in 3.4.

3.2.2 Sample of tutorials

The 25 tutorials used for this were found on a forum thread of a cryptomarket on Tor in late 2015. The thread revolved around links to free leaked tutorials, some written by established vendors or moderators. The user starting the thread had collated tutorials that had been leaked into the community from various sources, such as pastebin and Russian forums. The tutorials were leaked for free between 2013 and 2015. Some had already been available for sale before, so it is hard to determine when they were written exactly. One of the tutorials was, for example, a law enforcement agency’s insight into carders’ methods from around the time of early carding forums, such as ShadowCrew and CarderPlanet, between 2001 and 2004. The rest of the tutorials content is more recent, as some, for example, focus on Bitcoin laundering. The user starting the forum thread shared the tutorials for free, because some newcomers in the carding community were still charged high prices for the tutorials, even though they were already freely available on different forums and marketplaces.

The leaked tutorials in the forum thread focused on a wide array of topics. While most focused on carding, others topics ranged from the synthesis of various drugs to postal smuggling. To be included in my data sample, tutorials either needed to focus on the whole process of carding, laundering money from CNP fraud, delivering products from CNP fraud or technical security methods for carding. The tutorials that were selected thus focused on different facets of carding. While some only focus on terminology and basic methods, others focus on laundering via various cryptocurrencies and middlemen accounts. Some looked at the entire carding process, while others only zoomed in on one specific aspect.

Below, it can be seen on what topics the carding tutorials focused. The publication date refers to the date on the websites where they were found. While all were found in a cryptomarket forum post, there were links to different websites in this post where the files were stored. On these sites there were, in some cases, dates that predated the cryptomarket forum post. Asterisks behind the year indicate that the posting date of the forum post on the cryptomarket is the only known date.

#	Publication dates	Topic(s) of carding tutorials
I	2013	Glossary of carding terms; Common carding schemes;
II	2014	Ordering goods online with stolen cards; account take-over fraud; virtual machines; VPN; SOCKS5; burner phones; glossary of carding terms
III	2013	Glossary of carding terms; carding via eBay; carding via PayPal
IV	2013	Cashing cards; gift cards; VPN; Remote Desktop Protocol (RDP); Virtual private servers (VPS); SOCKS5; Spoof calling
V	2015(*)	Drops; MAC address spoofing; RDP; SOCKS5; Address verification systems
VI	2015(*)	PayPal; RDP; SOCKS5; VPN; Amazon Web Services
VII	2015(*)	Event websites; VPN; Cleaning cookies
VIII	2015(*)	CVV; Carding gift cards; SOCK5; VPN; Virtual credit cards; PayPal
IX	2015(*)	Tor; SOCKS5; PayPal; Virtual Machines; VPN; Online casino fraud

X	2015(*)	Bitcoin; PayPal; Ebay; SOCKS5; VPN; Amazon
XI	2015(*)	US credit cards; PayPal; Bitcoin; Middlemen accounts; Gateways; RDP; VPS; Phone spoofing; Cleaning cookies; Aging accounts; Alternative cryptocurrencies; Drops
XII	2015(*)	Long term carding schemes; Fullz; Documents; Anonymous virtual credit cards;
XIII	2015(*)	Address verification systems; Carding glossary; Verified by Visa; Bank identification number; Drops; SOCKS5;
XIV	2013	Bitcoin; CVV; SOCKS5; Domain Name System (DNS); Email accounts; Virwox; Moneygram; MtGox;
XV	2014	Bitcoin; CVV; SOCKS5; DNS; Email accounts
XVI	2015(*)	VPN; SOCKS5; UKASH; Open WIFI
XVII	2014	PayPal; Aging accounts; Middlemen accounts; Cashout accounts; Cleaning cookies; Virtual Machines; SOCKS5; Burner phones; Fullz; Documents; European accounts; Account verification; Bank identification number; Freelancer websites;
XVIII	2015(*)	VPN; Massively Multiplayer Online Games; PayPal; ICQ; Tor; Jabber; Bitcoin; Western Union; Perfect Money; Bank transfers; Chinese goldfarmers; SOCKS5; MAC Address spoofing; DNS; Name System; VPS; RDP
XIX	2015(*)	PayPal; Phone spoofing;
XX	2013	PayPal; SOCKS5; Middlemen accounts; Cash-out accounts; Anonymous visa; IBAN bank accounts; Documents; Freelancer websites;
XXI	2014	PayPal; SOCKS5; Documents;
XXII	2013	PayPal; Mailerbot; Fullz
XXIII	2014	Drops; Fullz;
XXIV	2015(*)	Drops
XXV	2015	Stripe; Fullz; CVV; Bank accounts;

Table 3.1 List of carding tutorials topics and publication dates

While some of these carding tutorials may be outdated now, they were still relevant to study, as it can be assumed that (aspiring) carders will first look at freely available tutorials to get familiar with the illicit trade. The sample is thus relevant to analyse, as these tutorials will have played a role in the learning process of carders. This represents a form of social learning and initiation into the carding subculture (Holt, 2007). A collation of free carding tutorials would, however, possibly be useful for all types of carders, as more experienced members can also use them to compare them to the efficiency of their own methods. The efficiency of some methods in the tutorials may be of uncertain quality or outdated. However, these tutorials were part of a collation and were widely shared before on a variety of forums and marketplaces. Many carders will thus likely have used these. Therefore, this collation of tutorials is sufficient to be used for the creation of a crime script of commonly advised methods for carding and cashing out.

Only free tutorials were analysed, as buying tutorials contributes to the thriving of underground marketplaces, which is ethically questionable. The data was obtained using the *Dark Web Monitor* tool by The Netherlands Organisation for Applied Scientific Research (TNO). The forum on which the tutorials were found went offline in April 2016. However, the forum posts were still accessible through the tool, as TNO had scraped all public forum posts on this forum, saved them in their tool and, consequently, made them accessible to browse for researchers. Without such socio-technical "web archival labour" efforts, through which access to "pre-existing" Web resources is preserved by organisations such as TNO, much of the Web would simply disappear (Ogden, Halford & Carr, 2017: p. 1). These efforts are socio-technical, as not all Web data that goes offline is simply automatically archived. Choices have to be made by agents involved in archiving what to archive, as active scraping efforts have to be ongoing to capture Web resources before they go offline. The forum posts in the *Dark Web Monitor* are ordered by language, topic and forums. I used the search term 'tutorials' and selected 'carding' as a topic. This led me to the repository of tutorials. The tutorials were analysed with a crime script analysis, which will be discussed in 3.4.

3.3 Interview data

3.3.1 Justification for using interviews

Cybercrime researchers often acquire their findings by, for example, quantitatively analysing marketplaces over time (Soska & Christin, 2015; Christin, 2013) or qualitatively analysing various aspects of forum posts on stolen data markets, such as buyer's feedback (Holt, Smirnova & Hutchings, 2016) and risk-reduction strategies (Holt et al., 2015). However, there is not much research on illicit online markets which obtains data directly from stakeholders, e.g. law enforcement, (incarcerated) cybercriminals, banks or customs. Some notable exceptions of research in which stakeholders are interviewed are Sheng et al.

(2009), Van Hout and Bingham (2013), Hutchings and Clayton (2016) and Kruithof et al. (2016). Sheng et al. (2009) interviewed a varied set of stakeholders: primary victims, infrastructure providers, for-profit protectors and public protectors to find countermeasures against phishing. Van Hout and Bingham (2013) interviewed one user of Silk Road, to get an in-depth understanding of the behaviour of a random user. Hutchings and Clayton (2016) talked to several people who run booter services, on which denial-of-service attacks are illegally sold. Kruithof et al. (2016) interviewed law enforcement experts, academics, forensic experts and custom officers to examine the Internet-facilitated drugs trade and to find information on detection and intervention practices. This research is most similar to Kruithof et al. (2016), with the main differences that it has focused on carding, not on drugs. Also, this research did not focus on the size of the illicit online trade, but will look at its enabling elements and how online criminals use tools, launder money and stay anonymous in this process. Furthermore, this research has looked into the response of law enforcement, banks and the payment card industry to such developments.

Semi-structured qualitative interviews were used. A set of questions and themes was prepared for the interviews, but a semi-structured style was used to allow for follow-up questions to interesting remarks made by the interviewees. Such a flexible approach was chosen, as this research tried to access information that “cannot necessarily be observed or accommodated in a formal questionnaire” and in this way a position is taken that values “people’s knowledge, values and experiences as meaningful and worthy of exploration” (Byrne, 2004: p. 182). Another interesting aspect of qualitative interviews is the fact that they can provide similar answers to questionnaires, but then with an unlimited range of answers and come with an accompanying context (Tewksbury, 2009). This is interesting when it comes to interviewees from law enforcement, the security industry and banking, as information about their processes of decision-making is normally limited to short press releases or judicial files. Moreover, in-depth conversations shine more light on how they decide on approaches for prevention, detection and interception.

3.3.2 Sampling

I have interviewed 14 experts during a period in The Netherlands in late 2016. In early 2017, during an internship at the INTERPOL Global Complex for Innovation in Singapore, where I worked in the Research & Innovation department, I had the opportunity to talk to five international law enforcement experts. For the interviewees in the Netherlands, I first contacted some people I met at a cybercrime conference in The Hague. They put me in touch with a cybercrime expert at a bank. Then, from his network and recommendations, I found more participants to interview. These experts were based at various teams at the National Dutch police, Europol and at other organisations, such as banks and card issuers. The last group of interviewees were found through my internship at INTERPOL. The requirements for being an expert were that they have extensive knowledge on the topics of carding and/or cryptomarkets. This meant that the interviewees should have at least three years of relevant experience. Experience in dealing with any type of fraud was also considered relevant. However, interviewees were only approached if that experience included at least three years of working on online carding and/or cryptomarkets. Initially, I hoped to talk to in between seven and twenty experts, depending on how much of their expertise the interviewees were willing to share with me. In the end nineteen experts were interviewed. See Appendix B for a full list of interviewees.

Purposeful sampling was used to find initial experts to interview. Purposeful sampling is used to select cases or individuals “from which one can learn a great deal about issues of central importance to the purpose of the research” (Patton, 1990: p. 169). Talking to experts was particularly useful for this research, as they are experienced in dealing with the research topic for several years and were able to explain how crimes on illicit online markets occur. Also, the experts were aware of measures that have been taken in the past, and can be taken in the future, to fight criminality on illicit online markets. Such qualitative information is invaluable for future research, as it can give the academic community insights which may not be obtained through analyses of marketplaces or other online methods. According to Holt (2017: p. 4), there is “no substitute for such information” from law enforcement. After an initial expert was found, I asked him for recommendations for experts he knew who might be willing to be interviewed as well. This practice of finding new participants is known as snowball sampling (Patton, 1990). Several of the interviewees were recommend several times by different initial experts, which showed that they are not simply good colleagues, but also considered experts by several people.

3.3.3 Coding of interview data

As all of the interviews, except for one, were recorded, verbatim transcriptions were made. Interviewees' comments were, however, not transcribed verbatim if the interviewee explicitly stated that a statement was 'off-the-record'. One interviewee did not want to be recorded, because he feared this might inhibit his anonymity. In this case, I relied on note taking, which I worked out immediately after the interview. A thematic analysis was used to identify patterns in the interview data. Comments of individual interviewees were given initial codes. Coding can help to improve the validity of qualitative data by showing that several interviewees mention the same issues or by collating categories of codes that can support emerging theories (Seale, 2004). The codes were mainly derived in an inductive manner, i.e. from the interview data. However, as the interviews were semi-structured, the questions may have steered several interviewees into the same direction. The coding scheme thus also partly appeared in a deductive manner, i.e. a sort of explanatory *verstehen* from pre-existing observations and readings. Codes across interviewees were collated, compared and merged if they overlapped. This process was repeated to end-up with a smaller set of themes. Finally, all the themes were refined again, to create a final set of overlapping themes.

Thematic analyses can both be conducted at the semantic and the latent level, which respectively focus on the explicit or surface meaning of interviewees' comments and on the underlying ideas and assumptions in the data. This thesis focused on the latent level, as it is interested in the "sociocultural contexts, and structural conditions, that enable the individual accounts that are provided" (Braun & Clarke, 2006: p. 85). This fits in with the overall Web Science approach of this work (see 3.6.1), as a thematic analysis at the latent level also allows for a more holistic approach that looks at the various facets that affect decision-making of both carders and law enforcement agencies.

3.4 Crime script analysis

The sampled tutorial data has been analysed to create a crime script analysis. The origins of this method in rational choice theory and situational crime prevention were discussed in Chapter 2 to understand its usability and validity in the context of online fraud with stolen payment card details. For this work, the tutorials were analysed for the topics they focused on. This list of topics can be seen in Table 1.4. A topic needed to be mentioned in at least three tutorials to be considered for the crime script analysis. This led to sixteen topics. The threshold was chosen as the crime script analysis would otherwise be too broad and lack focus, as the amount of topics would have almost doubled if the threshold of two tutorials would have been chosen, Therefore, these topics were selected to keep the script focused on recurring elements and on an "appropriate level of specificity" (Cornish, 1994: p. 153). Such an appropriate level is achieved when situational crime prevention measures can be designed, according to Cornish (1994). I believed these sixteen topics gave me enough insights into carding to design SCP measures.

Below, in Figure topics that were mentioned in more than three tutorials are listed.

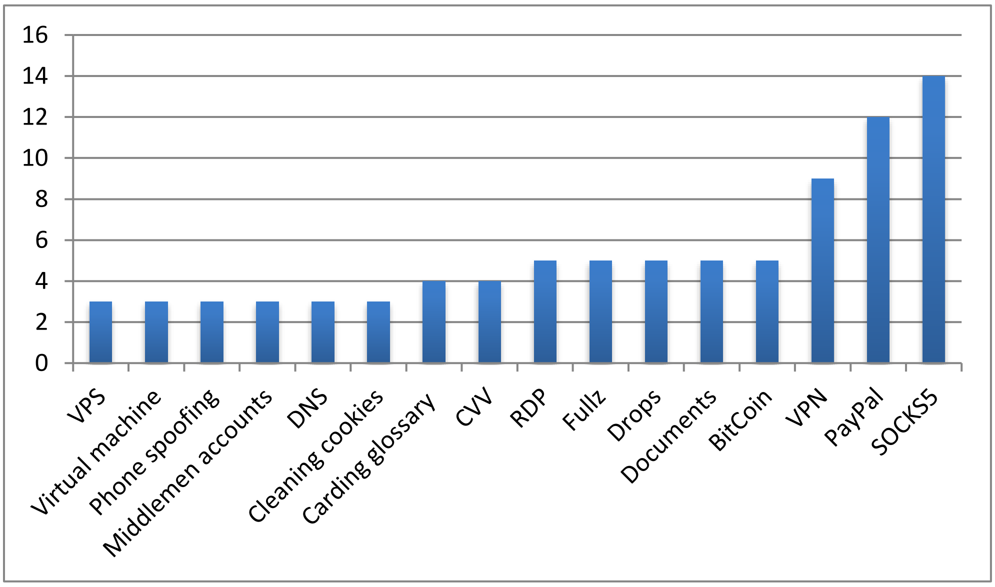


Figure 3.1 Mentions of topics in tutorials

After identifying the topics that were mentioned more than three times, I tried to subdivide the topics in scenes. Initially, as per Cornish' (1994) universal script, I tried to divide them into nine scenes. Hutchings and Holt did create such a universal script with the predetermined nine scenes for the online stolen data market. However, I found that such an approach based on the sampled tutorial data would lack focus, as it would become too broad and wide-ranging in its description. The 'instrumental' steps, identified by Cornish (1994), can in the case of carding be subdivided into other scenes, as will be shown in Chapter 4. Therefore, I decided to change the number of scenes to six: preparation, pre-entry, entry, pre-activity, activity, and post-activity. Several authors have previously altered the universal script approach to make it more crime-specific by creating clarifying schematic representations and diminishing the amount of scenes (Tompson & Chainey, 2011; Chiu, Leclerc & Townsley, 2011; Gilmour, 2014). Furthermore, the preparation scene was added without being explicitly discussed in the tutorials. However, because of the fact this preparation scene logically followed from the content of tutorials, it was deemed necessary to include, as the script would otherwise not be complete. This is further discussed in 4.1.1.

The crime script in this thesis is a planned script, which is a script characterised by its focus on the description of repetitive behaviour and is based upon intelligence (Borrion, 2013). This means that the actions have not necessarily been executed yet, but most likely will be in the future. In the case of carding tutorials it is likely that planned scripts, at least in part, are continuously being executed. This is the case, as forums are learning environments for users to obtain specialist knowledge on how to commit illicit transactions (Hutchings & Holt, 2015). Clear guidance on how to proceed, in a way that can keep one safe from external parties, is invaluable for potential users of illicit marketplaces and forums, as it can influence their decisions whether to engage in criminal activity.

For the crime script analysis in this research, the tutorials were used as a source of empirical data. The content of the tutorials was qualitatively analysed for recurring steps in the carding crime commission process. From this, a six scene process of carding emerged. While a larger amount of tutorials could have been analysed quantitatively, a qualitative approach was chosen as it provided more detailed insights into the specificities of the different methods described in the 25 tutorials. Various ‘tracks’ can be derived from all the tutorials to create a generalised but still variant script (Ekblom & Gill, 2016; Cornish, 1994). This will show the most common ways in which a crime can be committed. However, as will be shown later in 4.2.3, there might be dozens of tracks for certain crime types, which makes mapping them difficult. Therefore, further analysis with CommonKADS was needed.

3.5 CommonKADS and its origins

The crime script analysis in this work is extended on with an analysis of the tasks and organisation involved in carding with the CommonKADS method. As CSA maps out the most commonly taken paths in (online) offending, it largely overlooks deviations from the norms. The specific tools used in the offending process to accomplish a task need to be analysed in depth, as these may point to possible points for intervention. Particularly, when such tools are misused. A representation of the context and structure of carding is thus presented in Chapter 5 using the formalised organisation and task models of the CommonKADS method. This can create a better understanding of why and how carders use certain tools. Also, it will contribute to showing what the bottlenecks are in these tools. First, however, the origins of CommonKADS in knowledge engineering will be described. Second, the validity of CommonKADS’ models in the context of carding and its usefulness over other knowledge engineering will be explored. Finally, the models used to analyse the organisation, tasks and agents involved in carding will be presented.

3.5.1 Knowledge engineering

The discipline of Knowledge Engineering has over time focused on the development of information systems, in which knowledge plays an important role. Knowledge systems are traditionally used in the discipline of artificial intelligence and have been used to aid human problem solving. The goal of such systems has generally been to mimic the problem solving capabilities of (human) experts in a specific domain (Shadbolt & Smart, 2015). Knowledge engineering focuses on creating models from domain-specific knowledge. In this way, it creates a “purposeful abstraction of some part of reality” (Schreiber et al., 2000: p. 15).

As the ‘skeletons’ of the models are laid out in worksheets, knowledge engineering encapsulates formalised and reproducible methods that can be used to look at domain-specific knowledge and business processes. In this thesis, it has complemented the crime script analysis of Chapter 4 with a formalised analysis of the organisation of carders. It also showed what tasks and tools are used in which parts of the carders’ processes and lay bare what some of the bottlenecks in these tools are. By establishing this, it can be explored where carders are likely to deviate from the ‘optimal path’, which is established in the crime script analysis in Chapter 4. Looking for bottlenecks in transactions on underground markets on a formalised conceptual level can lead to new avenues for thinking about interceptive and preventive opportunities for law enforcement. CommonKADS is the structured knowledge engineering method that was used in this work.

3.5.2 CommonKADS

CommonKADS is used to look at the online illicit trade and abuse of stolen payment card details. There are a variety of other knowledge engineering approaches, such as MIKE, PROTÉGÉ-II and PROFORMA. These respectively focus on prototyping, ontologies and clinical expert systems in medical settings (Studer, Benjamins & Fensel, 1998; Batarseh, 2011). As there are many uncertainties in the online trade of stolen card details, such specialised methods are avoided and a more conceptual approach is taken, as it can better explain the specific domain. Moreover, CommonKADS allows for the mapping of context, which is important in understanding this domain. Also, its usage of the Unified Modelling Language (UML) models provides a broad reusable logical structure, which in combination with its focus on the modular level, i.e. structures, tasks and agents, allows the approach to focus both on the broad and the specialised elements of online payment card fraud.

CommonKADS is the most commonly used knowledge engineering method and enables researchers with the opportunity to represent knowledge in an implementation independent manner, which means that a knowledge-based system is not necessarily the outcome of the method (Studer, Benjamins & Fensel, 1998). This is useful in this work, as an abstraction of carding, with conceptual models that represent the structures involved in it, is the goal of using the CommonKADS method. Modelling in accordance with the CommonKADS method has previously been used to aid in improving a wide variety of 'real-world systems'. Examples of these include, but are not limited to, automated credit card fraud detection programs (Schreiber et al., 2000), emergency medical services (Post et al., 1997), breast cancer diagnosis (Sutton & Patkar, 2009), evaluating eyewitness identification (Bromby, Macmillan & McKellar, 2003) and situational awareness in humanitarian operations (Smart et al., 2005). As developing a knowledge system is thus not a necessary outcome when using CommonKADS models, its focus lies mainly on understanding the context of the organisation, tasks and agents. CommonKADS can be used to look at real-world situations by studying experts, users and their behaviour "at the workplace, embedded in the broader organizational context of problem solving" (Schreiber et al., 2000: p. 16).

3.5.3 Knowledge elicitation

To obtain the right representation of knowledge, a thorough process of knowledge elicitation is required. With the CommonKADS method, knowledge can be elicited from people, but also from textbooks, technical manuals, case studies and so forth (Shadbolt & Smart, 2015). The 25 tutorials, which are also used to create a crime script, will be used as 'knowledge'. Tutorials are similar to technical manuals, and can be to case studies as well as specific cases of crime commission are sometimes discussed within them. This is similar to following what experts do in a certain domain to create "meaningful structure and rules from the protocols", which in knowledge engineering is referred to as protocol analysis (Schreiber et al., 2000: p. 196). Typically, a protocol analysis involves following an expert while they are describing the problem-solving process. It can also involve an expert providing commentary on what another expert is doing. These methods are respectively referred to as 'self-reporting' and 'shadowing' (Shadbolt & Smart, 2015). The protocol analysis in this work is more indirect, as it looks at tutorials, which are descriptions of how to execute the cashing out process of stolen payment card details.

These tutorials are based on experiences of (experienced) traders of illicit goods on underground markets. Therefore, these tutorials can be seen as self-reporting, as the processes the writer of the tutorial goes through are meticulously described and based on experience. According to Schreiber (2000), a potential pitfall of protocol analysis is the difficulty to derive general domain principles from a set of protocols. However, prospective carders are also dependent on a limited set of tutorials, or ‘protocols’, making it hard to speak of general domain principles, as these will vary across forums, over time and between individual users. This means that a general ‘optimal path’, which will be shown in Chapter 4 with a crime script analysis, will often not be followed and deviations will occur. Therefore, protocol analysis is used at a broad level to get an overview of the methods and tools most commonly used in cashing out stolen payment cards. A general model has to be established before deviations from an optimal norm can be found. The knowledge elicited from tutorials will be conceptually modelled to understand the organisational and technical underpinnings of the processes carders go through to cash out stolen payment card data. By doing this, bottlenecks and deviations in this process can be found, which can be used to think about the apprehension of online fraudsters and dealing with broader issues of fraud. Organisational, task and agent models were used in this thesis to establish such an understanding of the processes carders go through.

3.5.4 Organisation, task and agent models

Organisation models in the CommonKADS method are used to look at the structure of an organisation and to explore the organisational context. It does this for finding problems in business processes and to help think about their potential solutions (Schreiber et al., 2000). The organisation model worksheets in this thesis give a high-level overview of business processes, aspects of the organisation and tasks from the perspective of carders. The information required to create these models was derived from the 25 analysed tutorials. The organisation models help in creating a better overview of the organisation of illicit marketplaces on which stolen payment card details are sold. They also show the significance of various tasks within carders' 'business processes' and can, based on this information, help to think of potential countermeasures against carding.

After modelling the organisational aspects of carding, the tasks involved in processes to cash out stolen payment card data will be mapped with task models. The goal of using a task analysis in CommonKADS in this thesis was to create a decomposition and analysis of all the tasks involved in carding. It zooms in on why a certain task is part of the 'business' process, how it is dependent on other tasks and looks, on a surface level, at what knowledge and competences are required for tasks in the process. The knowledge and competences required for the process are further explored in the *knowledge item worksheet*.

The *knowledge item worksheet* looks in-depth at the knowledge and competences required per task from the *task analysis worksheet*. As a model, it represents the knowledge needed to correctly execute tasks (Batarseh, 2011). More specifically, in the context of carding it can be used to get a proper understanding of how and why users of illicit online marketplaces use tools and services to stay secure while making profits from stolen payment card details. A goal of CommonKADS is to find 'bottlenecks' to help an organisation (Schreiber et al., 2000). In this analysis, however, bottlenecks are not found to help the 'organisation', i.e. carders using these methods for illicit purposes, but to think of strategies to reduce the efficiency of their illicit trade. The possible bottlenecks in tools used by carders are analysed with a review of the literature. Then, they are mapped in bottleneck models. These show the nature of the knowledge involved in a task and how this can lead to possible bottlenecks for either carders in their cashing out process or for law enforcement in their investigations.

The *agent model* is a rearrangement of other models from the point-of-view of agents involved in the transaction process (Schreiber et al., 2000). No new information is thus created for this model. The agent model focuses on the roles taken-up on a carding forum or marketplace. Because no new information is presented in the agent model, but only rearranged from organisation and task models, it is presented in Appendix A.

3.6 Methodology

3.6.1 Web Science

A Web Science perspective has guided the research, as it has studied the Web from an interdisciplinary point of view. Understanding the current state, growth and possible future of the Web has been a pressing concern that has led to the creation of Web Science. The original goal for Web Science was to "both understand the growth of the Web and to create approaches that allow new powerful and more beneficial patterns to occur" (Berners-Lee et al., 2006a: p. 769). In doing so, it takes the Web as its primary object of study and sees it as a complex socio-technical system that can only be understood with an interdisciplinary approach (Hendler et al., 2008; Berners-Lee et al., 2006b; Hall, 2011).

In Web Science both the social and the technical elements of the Web are analysed, as the "future of human society is now inextricably linked to the future of the Web" (Hendler et al., 2008: p. 68). The Web is not either a technological development or a social endeavour, but a complex network that is both social and technical (Tinati et al., 2014; Hall, 2011). To understand the development of the Web, the various contexts and motivations of actors involved in the Web need to be understood. Halford, Pope and Carr (2010) therefore extended the original proposal for Web Science by stressing the importance of adopting social sciences and humanities into Web Science. They emphasise that there are various important concepts from social scientific theory that can inform Web Science. Particularly relevant for this work is the co-constitution of society and technology.

The development of the Web is not unidirectional. While its technologies are created with a certain use in mind, a 'script', its use will most likely not be exactly as its creators envisioned it. This has been theorised as 'interpretative flexibility', which means that technological artefacts can have different meanings and be interpreted differently by different groups of people (Pinch & Bijker, 1989). Halford, Pope and Carr (2010) stressed its relevance for Web Science by arguing for the necessity of examining both how the Web impacts people and how people impact on what the Web becomes.

This is the case, as the Web is a part of society and thus co-constituted through "heterogeneous networks that are both challenging and re-producing older forms of inequality and producing their own varieties of inequality". Therefore, to include all actors implicated in the Web, the authors suggested that Web Science should adopt methods from disciplines that do not simply "validate themselves through appeal to objectivity and rationality" (p. 4). Web Science thus promotes approaches that move beyond measurements or positivistic attitudes and incorporates both the technical and the social. Such holistic socio-technical approaches appreciate the co-constitution of (Web) technologies by their technical elements, human use, effects on society and, conversely, society's influence on them.

Socio-technical Web Science perspectives have been used to guide a wide variety of types of research. Examples range from analyses of how socio-technical practices shape Web archiving (Ogden, Halford & Carr, 2017) to the socio-technical construction and practical use of Massive Online Open Courses (MOOCs) in higher education contexts (White & White, 2016) to the envisioning of Web Science as a basis for a new kind of digital literacy (Day, Carr & Halford, 2015). This work also benefits from taking a Web Science perspective, as it looks at the socio-technical practices of carding communities. The model created by Tinati et al. (2013, 2014) to understand the socio-technical growth of the Web can also help to explain the growth of carding communities. First, Web activities develop by multiple networks of heterogeneous actors (human and machine). Second, the networks gain actors, become stable, progress on its agenda and achieve agreed goals. The unorganised set of network participants become a mobilised network of activities. Finally, the success of the network leads to changes in other networks that have similar participants and goals, new networks are formed and existing ones re-arranged.

The relevance of using Web Science to study carding communities is thus apparent, as it allows for the socio-technical analysis of how carders facilitate their illicit trade. This thesis has strived to add to the discipline of Web Science by studying the socio-technical elements of carding communities in an interdisciplinary manner. First, 'optimal' paths of cashing out stolen card payment details were established, after which possible behavioural and technical errors in carders' decision-making were explored. For these analyses, methods from a variety of disciplines have been explored. While carders strive for anonymity, they, and the technologies they use, are not flawless. To analyse the trade in stolen payment details, the carders, the technologies they use and their interplay need to be understood. A socio-technical approach, a Web Science approach, was thus required.

3.6.2 Structuration, habitus and verstehen

Much research looking at cybercrime is focused upon quantitative measurements. This work, however, uses qualitative approaches to contribute to the research field, as it tries to understand how a relatively new form of crime occurs and how its agents and processes "operate in culturally-grounded contexts" (Tewksbury, 2009: p. 39). In doing so, it does not limit itself to one disciplinary perspective. While criminology is the most prevalent discipline in this research, several others are touched upon. Crime script analysis, a method from criminology, was extended upon with a knowledge engineering method that originates from the field of artificial intelligence, CommonKADS. Furthermore, various methods and theories from behavioural economics were used to further elaborate on some of the findings through the mapping of the organisation and task structure with the CommonKADS method.

The methods in this work are grounded in a methodology that gets its insights from the epistemological traditions of structuration theory and habitus. The methodology focuses on the importance of people's background, such as social groups they are a part of and (technical) experience. These are of importance in analysing how systems are constructed and the way agents act in such (online) systems.

Structuration theory simultaneously looks at structure and agency in the creation of social systems. It argues that structures and agents are not two binary entities, but that they are produced and reproduced in a duality of structure. In this duality, the contexts, rules and resources from which actors act and systems are produced need to be studied (Giddens, 1984). The way in which structure and agency are guided by their interdependence and contexts are of importance in this thesis. Habitus refers to the set of dispositions and structures that shape the way in which agents perceive the social world around them, produce meaning from it and act on it. According to Bourdieu, the interpretations of modus operandi through the individual logic of an agent can lead to resembling behaviour amongst individuals from similar backgrounds, but may vary across others. As Bourdieu has put it: “different conditions of existence produce different habitus” (1984, p. 170).

Human action is always a combination of structure and agency. It is thus both determined by society’s influence and agents’ inner will. While there is room for reflection on one’s actions, the setting, or social life, in which such actions occur grounds such reflexivity (Giddens, 1984). In other words, the actions and activities of agents are not made in a vacuum, but social groups and structures influence such behaviour. Furthermore, this work has attempted to include the notion of *verstehen* in its approaches. The notion of *verstehen* focuses on the subjective meaning of human action and takes contexts in which (criminal) actions take place into account (Weber, 1978; Ferrell, 1997). This has been seen as a necessity in explaining human (criminal) activity and is put in contrast to positivistic approaches, which often assume the predictability and causality of crimes (Young, 2004). For criminological *verstehen*, Ferrell (1997: p. 11) has argued, a researcher must develop an intimacy with illegality to understand the “situated logic and emotion” of crime. In the context of this thesis, particularly an *erklärendes verstehen*, an explanatory *verstehen*, is of importance. This also takes the broader context of meaning in consideration in its analysis. It does not take it directly from data without context, which Weber calls *aktuelles verstehen* (Weber, 1978). It thus does not simply look at the data, but situates it in a wider theoretical framework. In this thesis, the analyses exhibit the notion of *verstehen*, rather than presenting statistical analyses to interpret phenomena.

The tutorial data analysed in this work provides such an ‘intimate’ insight into possible decision-making strategies by carders, i.e. into their situated logic. CommonKADS models and the analysis of behavioural theories show that various contexts and cognitive biases often stand in the way of optimally following such recommended paths to anonymity in tutorials. Expert interviews with law enforcement, banking and security industry professionals were conducted to confirm the flaws in carders' paths in cashing out stolen payment card details. By getting a dual perspective from both data produced by carders and by experts whose goal is to minimise the efficiency of carding, a holistic perspective is used to understand cybercriminal decision-making.

Contextual factors are underexplored in cybercrime research. This work will attempt to contribute towards a better understanding of such factors. It will do this by mapping commonly advised paths in tutorials, exploring what the organisation and tasks involved in cashing out stolen payment card data are, finding possible bottlenecks in tools and exploring how cognitive biases can affect the decision-making of carders. Technical elements of tools will be taken into account and thus add depth to previous "technology-agnostic" work (Hutchings & Holt, 2015). Furthermore, expert interviews will be used to gain novel insights into cybercriminal decision-making and experts' responses to this. The exploration of these areas with interdisciplinary perspectives and unique data sources is what makes this thesis a novel contribution to the field.

3.7 Ethics

3.7.1 Ethical considerations for analysing carding communities

Researchers have to take various ethical considerations into account when designing research methods that analyse data from online criminal forums or marketplaces. Such environments often involve the offering of illicit goods and services. Researchers may observe negotiations on the buying and selling of such illicit products. Also, various types of information on users are available. However, because members of online criminal communities use pseudonyms instead of their real names, it is unlikely that a researcher will deanonymise a user when observing marketplaces or forums. Also, transactions will often be finalised in private discussions. So while a researcher might observe the initial contact between vendors and buyers, it will be harder to say with certainty that a certain crime was actually committed. Attributing crimes to specific individuals is thus complex for researchers of criminal communities. Traditionally, measures have to be taken by researchers protect the confidentiality of participants by, for example, removing names in the early stages of research (Israel, 2004). However, the participants themselves are already taking measures in the online context to hide their real identity, as they are aware that law enforcement agencies or other external actors may observe them, which could consequently lead to an arrest or reputational damage.

An ethically debateable practice that has been raised by Décary-Hétu and Aldridge (2015) is that researchers sometimes participate in the deception of forum participants by actively contributing to forum discussions or posing as a member of the community with illicit intent. Some researchers may go down such slippery paths, as certain forums and marketplaces are ‘invite-only’ and will only allow members in the community that prove to have cybercriminal experience or pay a fee. Generally, such practices are seen as unethical to study within the research community. This, however, does have the consequence that such marketplaces and forums within academia are not well-understood (Dupont et al., 2017). Passive observation of publicly available Web resources, i.e. lurking, seems to be the least ethically challenging research method. Still, it has been argued that forum members see lurking by researchers as intrusive and that it can therefore damage the sense of community (Eysenbach & Till, 2001). However, I would argue that in online criminal communities the presence of lurking external actors is already assumed. Such communities are aware that law enforcement will monitor their public forums and marketplaces, leading to the fact that they do not discuss personally identifiable information. The presence of lurking researchers will therefore, seemingly, be less of a concern for such communities.

According to Martin and Christin (2016), data analyses of cryptomarkets will not lead to higher risk levels for individual market and forum participants, as law enforcement agencies are already looking at them independently from academia. However, they do argue that research may highlight trends on such marketplaces to the public and law enforcement agencies, which could lead to increased targeting and prosecution of users in the community. This is, however, often even a goal of much research looking into online criminal communities, making it an ethical concern that will not apply to all types of research projects. A final ethical concern that can be raised when researching online criminal communities is the risk of the researcher becoming a target. Particularly, when researchers collect data with the purpose to deanonymise users and benefit law enforcement agencies' investigations, community members might feel threatened (Décary-Hétu & Aldridge, 2015). When the researchers' names are known, this could possibly lead to retribution in the form of digital attacks, such as denial-of-service attacks or defamation, or even physical attacks. No cases of actual physical harm to researchers due to their research into online criminal communities are known. Some researchers have even worked with pseudonymous members of such criminal communities through interviews in order to better understand their motivations (Van Hout & Bingham, 2013; Hutchings & Clayton, 2016). It can be argued that the purpose of the researcher is important in possibly becoming a victim of a community. Clearly stating one's intent, when it is not adverse towards members of the community, or observing a community in a passive manner are some examples of how such risks can be mitigated.

3.7.2 Ethical considerations for conducting expert interviews

This research was conducted in compliance with the British Society of Criminology Statement of Ethics for Research (British Society of Criminology, 2015). Ethical considerations are of importance for the interviews that I undertook. Particularly, informed consent and the limitations of confidentiality and anonymity were important to explain to research participants. Therefore, every time before I started an interview, I told the interviewee who I was and what my research was about. In this way, they were able to make an informed decision about participating (British Society of Criminology, 2015; Dexter, 1970). I also asked the participants' permission for using a digital recorder. If the interviewee preferred not to be recorded, which only happened once, I relied on note taking. If a participant said during the interview that information is 'off-the-record', I stopped taking notes (Dexter, 1970). Furthermore, I asked the participants whether they preferred to be anonymous. The British Society of Criminology Statement of Ethics for Research states that participants should also be informed about the limits to confidentiality and anonymity, as researchers in the UK can be subject to subpoenas if they have obtained evidence from research participants which could be of importance in a case. However, as I interviewed law enforcement officers and cyber security professionals, I did not believe this to be relevant for the expert interviews in my research.

3.7.3 Ethics approval

Ethical approval for the research conducted in this thesis was obtained from the University of Southampton's ethical board. Two separate applications were submitted, one for analysing tutorials and one for conducting expert interviews. The applications were eventually accepted, after resubmitting a couple of times, and can respectively be found in Appendix D and Appendix E. Below, I will briefly discuss some of the risks and issues that were discussed in these ethics applications and which I have kept in mind during the design and conducting of this research.

For the first ethical approval that was obtained, for analysing tutorials, there were several ethical issues that needed to be addressed. I stressed that participation of users of the cryptomarket I looked at was implicit and I did not approach participants directly, as I only collected the tutorials written by them. Furthermore, I stressed that I only collected the tutorials and no further personal details of victims, vendors or buyers in the community were recorded. Victims are 'present' in the community through their personal details and payment card data which are sold. Using deception, as described by Décary-Hétu and Aldridge (2015), is not a part of my research and thus not an ethical concern. I have also not paid for access to any forums or marketplaces, as it would have been unethical to contribute financially to an online criminal community. This is also the reason why I only looked at a (formerly) publicly available forum and at freely available tutorials, which I gained access to through a platform of TNO, which is discussed in 3.2.2. I have thus only lurked and not actively participated in any way. In the ethics application I have stressed that there was an extremely low risk of being attacked or targeted, physically or digitally, by community members but that I would contact the relevant authorities if I would notice it.

The first version of my ethics application for analysing tutorials was approved. However, before submitting it, I had been involved in the *Digital Police Officer* project, for which data from cryptomarkets was also collected. The ethics submission process for this project was more laborious, because of misconceptions by the ethics board about cryptomarkets in general and the risks involved in passively analysing such data, requiring several resubmissions and a meeting of project members with a member of the ethics board. According to

Halford (2017: p. 15), such misunderstandings can be ascribed to “radical transformations in our data landscape”, which may be complex to grasp by traditional formalised ethical processes. Perhaps because the *Digital Police Officer* project had set a precedent for analysing cryptomarket data at the ethics board, the subsequent submission for analysing tutorials for my thesis was immediately approved.

For the second ethical approval process, for analysing interviews, there were various other ethical concerns to think about. In this ethics application, which can be found in Appendix E, I explained how I would approach interviewees through snowball sampling, that I would ask them whether I could record the interview and that I would let them read a participant information sheet, after which they were given a consent form to sign. The participant information sheet contained information on what my research was about, risks being involved, benefits information, confidentiality information, an explanation of why the interviewee had been selected and contact details of my supervisor and the chair of the ethics committee. After reading this, the interviewee was given a consent form, in which they noted down whether they understood the research, its aims, were willing to participate and consent to being interviewed and recorded. In the ethics application, I said that I would collect signed consent forms and store them in an unmarked folder, which I have done. Interview notes were also stored in that folder. Furthermore, I promised, once this research is over, to destroy consent forms and notes, if they carry identifying information. The ethics application was not immediately accepted for the interviews, as I initially proposed to also interview (arrested) members of carding communities. After discussing this with the ethics committee and interviewees from law enforcement agencies, I abandoned this idea because of potential ethical ramifications and accessibility issues.

3.8 Limitations

3.8.1 Possible limitations of tutorial data

There are various possible limitations to the use of tutorials found in a carding community. The first limitation is that the provenance of tutorials is often difficult to ensure. Tutorials are sometimes reposted or resold several times. In this thesis, the publication date of the tutorial, if one was present, was used to verify when it was written. However, in some cases there was no date and the posting date on the cryptomarket forum had to be used. For some tutorials, it was stated that they had been available for a price before, but were now posted for free into the community as the information had been resold by vendors for too long. The methods of carders have changed over the years and therefore it is most relevant to analyse recent tutorials, as understanding their modus operandi can contribute to thinking of countermeasures by law enforcement and industry. As there was uncertainty over the exact publication date of most tutorials, I did not do an analysis of the evolution of carding methods, which Vidal & Décary-Hétu (2018) have done for methamphetamine production. However, there is also value in analysing tutorials that are older or have an uncertain date, as these are still the ones that are encountered by carders and are more likely to be freely available.

A second limitation of the used tutorials in this work is that it cannot be established how many carders have used them. While it is likely that many have accessed and used them, there are no statistics available. On some marketplaces statistics on sold products are provided. However, these tutorials were offered for free on a forum and statistics were therefore lacking. Third, as the tutorials were collated and reposted, it cannot in every case be established who wrote the tutorials. Some tutorials were written by established users, but others did not specify who wrote them. In theory, law enforcement or other users with intent to deanonymise carders could even have planted the tutorials. However, this is most likely not the case, as experienced members of the carding community reposted the tutorials, from which can be assumed that their purpose was to strengthen the community instead of deanonymising individual users.

It could be argued that the usage of 25 tutorials is a limit as their content will not be generalizable to account for all kinds of behaviour by carders. Critics could argue that a larger quantitative study of tutorials or court documents could provide a more general insight into the decision-making of carders. However, I believed that a qualitative approach would provide a more in-depth perspective, which can better account for perspectives on cognitive biases and contextual factors. Critics could also argue that the quality of the content of tutorials is often questionable. While this may be true, the analysed tutorials were widely shared and it could therefore be argued that many carders will have seen them and, at least, have been influenced by them. This justified their usage in this study. Furthermore, I believe that the usage of tutorials, more generally, can be defended by the fact that it is new data that is "free from the bias of criminal justice derived data" (Décary-Hétu & Aldridge, 2015: p. 128). While there are some limitations in their usage, studying them can lead to novel insights into the operational security of carders.

3.8.2 Possible limitations of expert interviews

A limitation on using expert interviewees from law enforcement, banking and the security industry on the decision-making of carders is that these interviewees are not carders themselves. While they can provide insights on their personal experiences in dealing with carders, they can only represent their own observations, which will not necessarily be representative of all actors on online forums and marketplaces (Kruithof et al., 2016). In this manner, it is a 'proxy' on the decision-making of carders. A combination of interviews of carders and experts from law enforcement, banking and security industry might have been an ideal approach. However, as the University's ethical committee did not accept my application to interviewing carders and some contacts at a Dutch law enforcement agency told me that even they had issues with talking to carders, I abandoned this idea. Still, the views of expert interviewees in this work are unique insights that complement previous research. This is the case, as such expert views are generally not widely publicised, because of the secretive nature of their work. To deal with this limitation, I did not only ask them about their insights on the decision-making carders, but also on what the issues are they encounter at their agencies in dealing with carding and other cybercrime.

Another limitation of interviews with law enforcement and security industry experts was their potential lack of willingness to share some of their knowledge, as it may be classified information or part of tactics which they do not want to be published and publicly known. This is the case, as it may undermine their ability to covertly do their work and may alert cybercriminals into changing tactics, for example, by picking up tools that better hide their illicit activity. Therefore, agreements with experts had to be made about whether I can use everything they say in the interviews. If they, for example, accidently gave away information that should not be made public and correct themselves, I had to comply with these wishes. A more general concern surrounding expert interviews was whether the experts are experienced enough, i.e. not all experts have equal levels of knowledge and can (accidentally) provide false information as well (Dorussen, Lenz & Blavourkos, 2005). However, with this issue was dealt by using a snowball sampling method, as described in 3.2.2.

A general concern of qualitative interviews is their focus on depth rather than breadth, which leads to a limited generalisability (Tewskbury, 2009). However, generalisability has not been the goal of this research. Its goal in using interviews was obtaining a more in-depth understanding of what the perception of usage of tools by carders is at law enforcement agencies, security companies and banks. Furthermore, its goal was to discover to what extent these measures by carders complicate their detection and prosecution. This contributed to the current academic literature, as such accounts from law enforcement and industry are lacking, particularly when it comes to carding, cryptomarkets and how these affect policing.

3.8.3 Possible limitations of crime script analysis

Crime scripts do not show all the possibilities in which crimes can be committed. Still, a scripting approach is considered useful for identifying the most significant steps of criminal operations, which can lead to an illumination of ‘structural choke points’ (Leontiadis & Hutchings, 2015). Structural choke points are described by Leontiadis (2014) as parts of the criminal operation that are crucial for criminal profits and can, once targeted properly, lead to a reduction in opportunities and incentives to engage in such criminal operations. The removal of key brokers, according to Leontiadis, can lead to a major disruption in online criminal environments. However, a major issue is that not every important facilitating element in criminal operations is illegal. This makes it questionable to what extent such choke points can be targeted, as they may have a far-reaching influence and use outside of cybercriminal environments. This is, for example, the case with proxies, anonymity tools and cryptocurrencies.

While a crime script approach can clarify commonly recurring elements in the crime commission process, there are various other limitations stemming from the original work by Cornish (1994). Several authors have picked up on these limitations and tried to suggest improvements. Because scripts are often crime-specific they tend to be tentative and of limited generalisability (Chiu, Leclerc & Townsley, 2011; Tompson and Chainey, 2011; Lavorgna, 2013; Lavorgna, 2014; Hutchings & Holt, 2015). This is amplified by the fact that scripts are often based upon small sample sizes. Ekblom and Gill (2016) believe that the scope of crime script analysis should be focusing more on the broader dynamics of offending instead of a “detached and narrow” decision-making model (p. 335). They accept that crime scripts might not lead to preventive proposals then, but they argue that the practical benefits could improve over time. Holt et al. (2015) have acknowledged that crime research should not only be crime-specific, but also context-specific, as context may affect steps in the crime commission process. In this research, attention is given to such contextual factors to mitigate this limitation of crime script analysis.

Hutchings and Holt (2015) have questioned whether crime scripts can be created from tutorial or criminal forum data, as law enforcement agents or others might be active on the forums for investigations. However, it is unlikely that law enforcement will make up a significant part of a forum’s user base and comments, because of the capacity and resources this would require. As the limitations of crime script analysis, and situational crime prevention, are an important part of this thesis, they are further discussed in Chapter 4. Throughout this thesis, it is argued how theories from behavioural economics can complement crime script analysis.

3.8.4 Possible limitations of CommonKADS

The usage of experts for knowledge elicitation can be seen as a possible limitation for the CommonKADS method. Particularly when a limited number of experts or experts from the same company or institution are used for knowledge elicitation, the dataset obtained may be biased. This can be the case, as all experts may show the same working patterns. A varied set of experts thus ideally needs to be used for knowledge elicitation. A possible issue with protocol analysis is that experts may describe the process differently from how it is performed (Schreiber et al., 2000). Self-reporting may thus not be accurate.

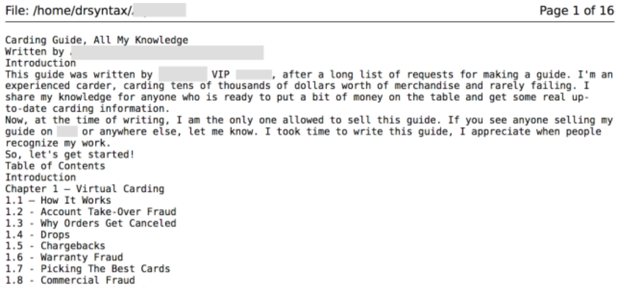
This is a limitation which can be resolved by shadowing an expert. However, in the context of carding, this is a clear limitation. Looking over the shoulders of carders while they try to cash out stolen payment details seems an impossible task for researchers, both because of ethical ramifications and access issues. Therefore, ‘self reporting’ of carders in tutorials was used in this research for analysing their behaviour.

Chapter 4 A crime script analysis of carding

In this chapter, a crime script analysis of how online fraudsters use stolen card data is presented. In doing so, it has looked at the applicability of crime script analysis to an online environment. More specifically, by applying the method to the domain of carding, it intended to find the steps carders take to obtain and cash out stolen payment card details and how these steps can contribute to the creation of measures for prevention. A crime script analysis of carding, based on 25 tutorials, was presented. Situational crime prevention measures were also derived from the script. While it appeared that a crime script analysis can be used to create possible prevention measures, the effectiveness of these situational crime prevention measures was also questioned at the end of this chapter.

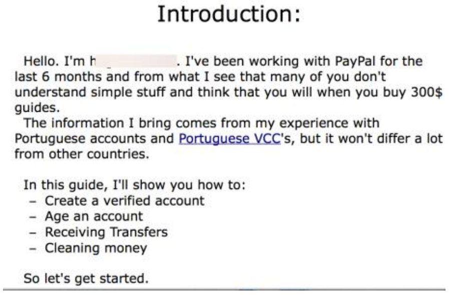
4.1 Crime script analysis of tutorials

To create a planned script, 25 tutorials were analysed. Below, some screenshots of the analysed tutorials are presented.



File: /home/drsyntax/[redacted] Page 1 of 16

Carding Guide, All My Knowledge
Written by [redacted]
Introduction
This guide was written by [redacted] VIP [redacted], after a long list of requests for making a guide. I'm an experienced carder, carding tens of thousands of dollars worth of merchandise and rarely failing. I share my knowledge for anyone who is ready to put a bit of money on the table and get some real up-to-date carding information.
Now, at the time of writing, I am the only one allowed to sell this guide. If you see anyone selling my guide on [redacted] or anywhere else, let me know. I took time to write this guide, I appreciate when people recognize my work.
So, let's get started!
Table of Contents
Introduction
Chapter 1 – Virtual Carding
1.1 – How It Works
1.2 - Account Take-Over Fraud
1.3 - Why Orders Get Canceled
1.4 - Drops
1.5 - Chargebacks
1.6 - Warranty Fraud
1.7 - Picking The Best Cards
1.8 - Commercial Fraud

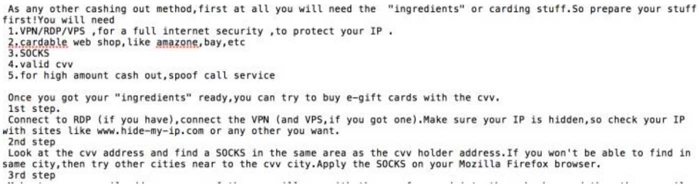


Introduction:

Hello. I'm h[redacted]. I've been working with PayPal for the last 6 months and from what I see that many of you don't understand simple stuff and think that you will when you buy 300$ guides.
The information I bring comes from my experience with Portuguese accounts and Portuguese VCC's, but it won't differ a lot from other countries.

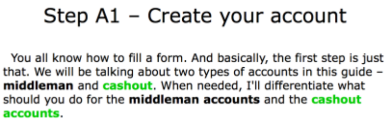
In this guide, I'll show you how to:
- Create a verified account
- Age an account
- Receiving Transfers
- Cleaning money

So let's get started.



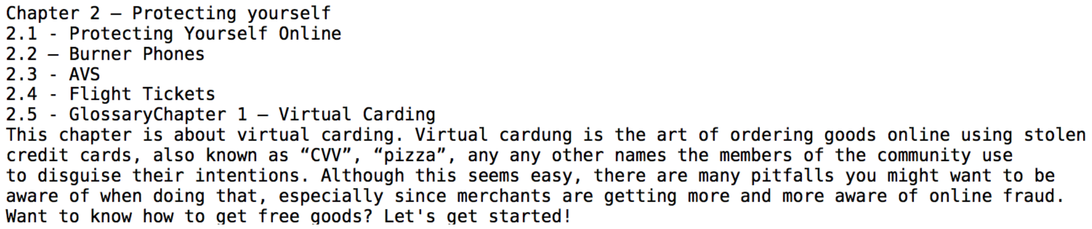
As any other cashing out method,first at all you will need the "ingredients" or carding stuff.So prepare your stuff first!You will need
1.VPN/RDP/VPS ,for a full internet security ,to protect your IP .
2.cardable web shop,like amazone,bay,etc
3.SOCKS
4.valid cvv
5.for high amount cash out,spoof call service

Once you got your "ingredients" ready,you can try to buy e-gift cards with the cvv.
1st step.
Connect to RDP (if you have),connect the VPN (and VPS,if you got one).Make sure your IP is hidden,so check your IP with sites like www.hide-my-ip.com or any other you want.
2nd step
Look at the cvv address and find a SOCKS in the same area as the cvv holder address.If you won't be able to find in same city,then try other cities near to the cvv city.Apply the SOCKS on your Mozilla Firefox browser.
3rd step



Step A1 – Create your account

You all know how to fill a form. And basically, the first step is just that. We will be talking about two types of accounts in this guide – **middleman** and **cashout**. When needed, I'll differentiate what should you do for the **middleman accounts** and the **cashout accounts**.



```
Chapter 2 – Protecting yourself
2.1 - Protecting Yourself Online
2.2 – Burner Phones
2.3 - AVS
2.4 - Flight Tickets
2.5 - GlossaryChapter 1 – Virtual Carding
This chapter is about virtual carding. Virtual cardung is the art of ordering goods online using stolen
credit cards, also known as “CVV”, “pizza”, any any other names the members of the community use
to disguise their intentions. Although this seems easy, there are many pitfalls you might want to be
aware of when doing that, especially since merchants are getting more and more aware of online fraud.
Want to know how to get free goods? Let's get started!
```

h[redacted]'s PayPal Guide

Screenshots from various tutorials

From a crime script analysis of the 25 tutorials, the following six scenes were derived as the most commonly advised process when carding:

1 Preparation - Get familiar with environment

2 Pre-entry - Security before entry

3 Entry - Buy stolen cards

4 Pre-activity - Find ‘cardable’ websites

5 Activity - Cash out cards

6 Post-activity - Security and reputation afterwards

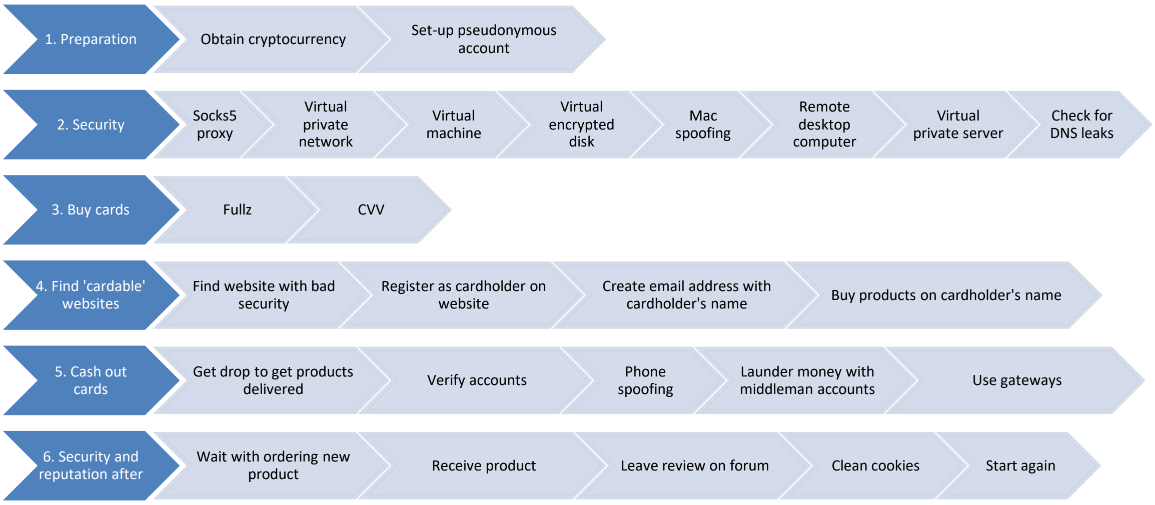


Figure 4.1 Crime script analysis of carding

4.1.1 Preparation – Get familiar with environment

This first step is the only essential part of the transaction process that is not described in tutorials. However, it can be logically deducted from the tutorials. This is the case, as at the point when a user reads one of these tutorials, certain steps will already have to been taken. Initially, before the actual process of buying stolen payment card details starts, potential carders will have to get familiar with the environment they are entering. Before they will have access to tutorials, they will have to have found the right forums to buy card details. Also, they will have to have obtained the right (crypto)currency to pay for the cards and, optionally, a tutorial, if it is not provided for free.

Before a vendor of stolen card details is approached, a buyer will have to set-up an account with a pseudonymous username that cannot lead back to their real identity. Online identities are the brand of a cybercriminal, particularly for vendors, and there is therefore an incentive to build-up a strong reputation with one identity (Lusthaus, 2012). On the other hand, law enforcement mainly targets high-profile cybercriminals, which feeds the incentive for users of illicit forums to change their usernames regularly to stay as anonymous as possible. This has led researchers to try to profile users based on, for example, analysing writing style with linguistic analysis, which has been an aim of *the Digital Police Officer* project at the University of Southampton (van Hardeveld et al., 2015; Webber et al., 2015) and other research initiatives (Afroz et al., 2014).

4.1.2 Pre-entry – Security before entry

Throughout the process of carding there is one crucial element that ties all the other steps together and can lead to serious consequences for a carder, if executed wrongly: security. It is generally strongly advised to members of underground communities to get their operational security in order before they start the process of obtaining cards. More specifically, it is regularly recommended to carders to protect their physical computer by using a virtual machine for anything carding-related. As stressed in tutorial II:

> “The VM (Virtual Machine) is an installation of Oracle VirtualBox or VMWare, whatever you prefer. It's like a computer in your computer. Your computer is the “host machine” and your VM is the “guest machine”. In your guest machine, put everything related to carding. Never put anything fraud-related outside this VM. Keep everything at the same place, you don't want to leave proofs on your computer.” [II]

By creating a virtual encrypted disk with a virtual machine on it, everything is encrypted when the computer is switched off. In tutorial 2 it is mentioned that this is particularly useful when law enforcement raids one’s house. In the case of such an event, the computer’s plug can quickly be pulled and there will be no simple way to access evidence on it anymore, as its data will all be encrypted.

> “By using TrueCrypt, you ensure that your VM is all encrypted, and that everything related to carding “vanishes” when the power is switched off, and you need to decrypt the volume again to access it. So if LE barges in your house, pull the plug on your computer, and all proofs are gone.” [II]

Remote Desktop Computers (RDP) and Virtual Private Servers (VPS) can also be used, according to various tutorials. These are used by carders to access someone else's computer and to thus make it seem as if the carding-related activity is being done from that computer. This is generally advised, as other IP addresses are then used and one's own is obscured. In some tutorials these tools are merely mentioned as an optional step, but other tutorials call it crucial.

> "Alright so let's get started, the first thing we're going to need is the RDP/VPS. In layman's terms a VPS/RDP is basically another computer that's hosted somewhere else. You're going to use these as the personal computer to open the paypal accounts. [...] **ALWAYS!!** Connect to the rdp/vps through a security barrier; never connect using your own isp!!" [XI]

Vendors on various marketplaces on Tor offer these tools[23]. They can be bought with cryptocurrencies, which adds another layer of protection. This is especially the case when so-called mixing or tumbling services are used to mix-up transactions with other users' coins to further obfuscate where the coins originally came from. It is also recommended in two tutorials to spoof the MAC address of one's computer, to pretend it belongs to another device on a network.

> "A minimal use of protection is spoofing your mac address, and then connecting to open wifi. Yes,spoof the mac of your computer. Why? Because wifi can log mac addresses that log onto their connection. You don't wanna be the odd man out when it comes to your safety, do you? No. You don't." [V]

Another important security step, which is mentioned in almost every tutorial, is the use of a virtual private network (VPN). A VPN is a private network that uses "public networks (such as the Internet) tunnelling protocols, and security

[23] In August 2017

procedures to tunnel data from one network to another" (Hawkins, Yen & Chou, 2000: p. 134). VPNs make a user's traffic appear to come from the VPN host. Therefore, VPNs are used for remote working, so it appears that the employee is located within the network of a company. They are also used to create private, encrypted and secure connections to avoid government censorship and to access content from countries in which it is not blocked. According to some tutorials, a problem with VPNs is that merchants can see when someone using their services is using a VPN service. If a defrauded party contacts law enforcement and if they, in turn, contact the VPN provider, they can often still get access to a fraudster's browsing habits. Merchants might also blacklist some VPNs that have been used for illicit behaviour before. However, it is still seen as an extra layer of protection and recommended within the underground community.

Some tutorials recommended using a SOCKS5 proxy on top of a VPN to get around the blacklisting. It is generally not advised to use public SOCKS5 proxies as they might have been used for illicit purposes before. To use a SOCKS proxy, a user enters the IP address and port number of the proxy, which can be found in proxy directories online, into a configuration screen of the browser (Roberts et al., 2010). SOCKS proxies are sometimes offered per city and can thus make it seem as if a user is from that city, as the IP address will be located there. Carders therefore also use SOCKS5 proxies in a later stage of the process to impersonate the cardholder. They do this by setting their location in the vicinity of the home location of the cardholder while using the stolen card details. This is used to trick fraud detection systems, which may not notice a deviation from regular payment patterns, as the cardholder is impersonated and it thus seems as if payments are being done from the same location.

> "Enable VPN + Socks less than 100km from the city linked to your CC." [X]
>
> "After deciding which cvv you're going to use on the shop, you need to get behind a socks that is as CLOSE to that city as possible." [V]
>
> "Be sure to chain a regional socks5 with your Tor connection so you appear to be from the same country that the cardholder is in" [XIV]

When additional security measures are in place, it is recommended in some tutorials to members of the underground community to check whether their domain name system (DNS) is leaking. If any traffic does not go through the secure connection, a snooping party can log it. This can be checked by doing an online DNS leak test in which can be seen whether one only uses the DNS provided by the anonymity service and not the original one belonging to one's own computer. Furthermore, connecting to open Wi-Fi is recommended in a tutorial. Finally, it has been advised to potential carders to clean their cookies before becoming active, with cookie cleaning programs even being mentioned as an alternative to virtual machines.

4.1.3 Entry – Buy stolen card details

Once a carder has set-up an account, obtained the right cryptocurrencies and security measures are in place, stolen card details will be bought as a next step in the process. Card details are often acquired by vendors through data breaches at companies, key loggers, phishing scams or by physical skimming of ATMs (Hutchings & Holt, 2015). They are then sold on carding forums, which can be found both on the 'regular' web and on hidden services on the Tor network. This crime script analysis looks at the steps taken after card details are offered on such forums and marketplaces. Cards from a wide variety of countries are offered and will be priced based on their 'freshness', i.e. how recently they have been illegally acquired by the vendor. The most commonly offered products are *CVV* and *Fullz*, the first specifically focusing on all the details on a payment card, such as the card number, expiration date and cardholder's name, while the latter generally includes all the information on an individual needed for fraudulent purposes, such as date of birth, mother's maiden name, home address, email address, phone number and so on. Sometimes the two are sold together. Card details are offered checked or unchecked, which shows whether the vendor has already tested whether the products work for fraudulent purposes. In one tutorial it was recommended to always purchase card details as untested, as the fact that they have already been used might have led to the card being blocked, as the cardholder or issuer might have noticed the irregular activity. It is also recommended in several tutorials to buy cards from established or 'fullz' vendors.

> “Buy from a respected vendor” [XVIII]

> “[…] select only the cards where you can have full information. This is my trick to get only good cards. Of course, the best option is to find a fulls vendor, but there are not a lof of them, so escalate your cards the way you desire.” [II]

4.1.4 Pre-activity – Finding ‘cardable’ website

After stolen card details are obtained, carders will try to get as much profit from the cards as they possibly can before they get ‘burned’. Cards are burned when the issuer blocks them after cardholder and/or the cardholder’s bank found out about the illicit use of the card. The security measures of the websites where they try to use the stolen card details are an important consideration for carders, i.e. checking how ‘cardable’ they are. Contrasting advice is given on this matter in various tutorials. Some argue that it is best to try and move away from large online retailers, as the smaller ones will have less security procedures in place. For example, they may not use a 3D Secure method, such as ‘Verified by Visa’, for which a password has to be used as an extra step of security. On the other hand, smaller businesses might contact law enforcement more quickly after they notice a loss, whereas large retailers might just take the loss as they might see the process of contacting law enforcement as too time-consuming, as stressed by II:

> “Some big merchants like […] and […] will just eat the loss and assume that they failed at fraud detection, but smaller merchants will make a formal complaint at their police department.” [II]

> “You're going to need to find shops that are weaker, have less security for fraud prevention. Don't just jump in and start scrolling through sites like […], and […]. They're not stupid, they know their stuff. You need to look for sites that aren't popular. Maybe try and steer away from the most commonly stolen items at first, like electronics. Try for clothes, smaller stuff, get creative here folks. Browse around on google for those shops

> that you've NEVER heard of before. Look for those tiny, unpopular weak sites.” [V]

Registering as the cardholder on online retail sites is an essential step for carders, according to various tutorials. If they have all the right details in place, it is less likely that an online retailer’s security team will notice irregular behaviour, as these have algorithms merely in place to check whether the details on the account match the information on the cardholder. Some carders complement the full information they have on the cardholder by forging the location of the cardholder with a SOCKS5 proxy, which will be set close to the location of a cardholder. In this manner, irregular spending patterns may not be noticed by the cardholder’s bank, as the location appears to be the same as regular transactions. It is advised in the tutorials to launder the money through as many ‘middlemen’ and ‘gateways’ as possible. Middlemen refer to a variety of accounts owned by the carder from which money should be transferred from one to the other. However, this should not be done directly, as the accounts may be linked to the carder more easily then. Therefore, gateways are used, which are services on which the carders also set-up multiple accounts and then make ‘transactions’ with themselves. In this way, it seems as if there was a legitimate transaction, but in fact the carder will never buy anything. Such laundering methods are part of the cashing-out process.

> “you post with your cashout account some kind of service (translation, for example) and you buy the service with your Middleman account. It will take some time in the beginning - new members on freelancer websites cannot cashout as quickly as you'd like – but at least the money is clean, right?” [XVII]

> “[…] make invoices/products through a third party gateway such as […] etc or making your own ecommerce website. There’s literally 100’s, if not 1000’s of gateways online we can use to do this. […] a gateway is a way to clean the funds from credit card to the middle man account.” [XI]

4.1.5 Activity – Cash out cards

The way in which carders look for 'cardable' websites partly depends on what they want to gain from the stolen card details. Before the card gets 'burned', carders will try to obtain physical goods, money, services or vouchers. Money, services and vouchers can generally all be dealt with 'virtually', i.e. nothing has to be dealt with in person. However, when ordering physical goods, the carder will need a 'drop' in place.

Drops

A drop is a place where a carder can send goods that were obtained with stolen card details. Drops are (empty) houses, post boxes or other places used for the delivery of illicit or illicitly obtained goods. It is stressed strongly in several tutorials that the drop address cannot have any links to the carder's life, but should be far away from one's home address. Sometimes abandoned houses are used. Another recommendation is to set-up pick-up schemes, which involves the carder hiring someone to pick-up packages, a 'packet mule' (Europol, 2016), and to drop it in yet another location where the carder can then pick it up. One tutorial even recommended carders to create a fake company that says to hire people to reship packages:

> "The point here is to make an ad as a reshippin company that is lookin to employ new people and get them to work asap." [XXIV]

This extra step can make the package, and thus the carder, even harder to trace as finding out the address of the first drop will also not be useful for law enforcement then. However, with such a service, the person who picks up the packages will know the final drop-off location and will thus be an extra security 'flaw' to think about for the carder. It is advised in tutorials to never actually meet in person with the pick-up person and to let them drop-off the package at yet another drop address or otherwise save location. Some markets on the Tor network have previously offered the 'dead drop' model, in which a vendor leaves a package in a physical location and sends the buyer the geographical coordinates and a video of leaving it there (Aldridge & Askew, 2017). Another proposed method involves sending a package to strangers, for example randomly selected in a telephone directory so they can be called, informed about the ‘wrong delivery’ and the package can be picked up.

Physical items and PayPal

Carders use stolen payment card details to obtain a wide variety of goods. The most popular items according to one tutorial are electronics, such as computers, laptops, tablets, televisions etc. According to Europol (2016), airline tickets, car rentals and accommodation are also often paid for with stolen card details. Furthermore, it is advised to make orders look legitimate and ordinary. For example, the use of gift-wrapping was recommended in a tutorial. Also, it was stressed that (prospective) fraudsters should not spend too much on products in one go, as this may alarm merchants or card issuers. To order physical items from online retailers, it is often advised to use PayPal as a payment method. Carders should first create email addresses on the cardholder’s name, to open the PayPal account with. Furthermore, it is advised that carders have a variety of information about the cardholder available, such as card details, social security number and scans of various documents. In this way, they can make it appear as if the account is actually created by the cardholder.

It is recommended in tutorials to verify PayPal accounts, as this leads to optimal use, i.e. looser restrictions on the sending of money and on receiving limits. According to PayPal, verification leads to an increase of “trust and safety” in its community[24]. In tutorials, there are many tips on how to verify accounts which are set-up with cardholder’s details. Phone spoofing is used sometimes to present the area code of the cardholder to the bank, to make it seem as if the phone call comes from the right geographical area. In such phone calls, security questions will be answered, which the carder might be able to answer with the obtained information and scanned documents about the cardholder. To make the carder’s illicit transactions seem even more legitimate, it is advised to ‘age’ their PayPal accounts. The process of aging involves sending some legitimate funds through the account. The longer this goes on before any illicit transactions are made, the more amounts of dirty money can be send through at a later stage.

[24] https://www.paypal.com/pt/webapps/mpp/security/buy-verificationfaq?locale.x=en_PT

> "The more transaction history and age your paypal account has the more it can handle in receiving funds! Ideally aging the accounts for a month or more would be best but if you're on a time constraint 1 week would be ok. As far as transaction history it would be best to run $500-$2000 of clean funds through the account spread across a month. Of course this is not necessary but it does make a big difference." [XI]

Laundering money

Middlemen accounts are used on payment systems, such as PayPal, to launder money. It is advised in tutorials to use one IP-address per account. This makes it seem as if the accounts actually belong to different people in different locations. If all the transactions are made from and sent to the same location, the security algorithms might pick this up, as payments normally come from various locations. SOCKS5 also has to be used by the 'buyer', as the carder's IP-address has to match the cardholder's location. VPN and Tor should not be used, as some payment systems can detect this, according to one tutorial. Furthermore, it is advised in another tutorial to use a dedicated browser per account. In this manner, there is a smaller chance of accidently using the wrong account for certain tasks. The multiple accounts can be used to launder money in a wide variety of ways. Such methods are not specific to PayPal, as these are also used with other payment providers. Some examples of common ways in which carders launder money from cardholder's accounts, as described in various tutorials, can be seen below in Table .

Launder method	Description
Creating fake events on websites of ticket sale companies	- Create event that will not actually take place - Set price of tickets - Buy own tickets with stolen card details, not more than two per card - Send money to own account
Converting money to cryptocurrencies	- Buy coins from an alternative cryptocurrency (i.e. different than Bitcoin) with stolen card details - Transfer alternative coins to Bitcoin - Optional: use bitcoin mixer to make origin of coins harder to trace - Optional: transfer Bitcoin to regular currency and into

	carders' bank account
Freelancing sites	- Create several accounts on freelancing website - Use different IPs and email addresses per account - Make job with one account - Fill the 'vacancy' with other account - Pay 'freelancer' with PayPal or wire transfer
Gift cards	- Create, verify and age PayPal account on cardholder's details - Buy gift cards on gift card websites - Resell gift cards - Receive money on bank or PayPal account

Table 4.1 Various laundering methods recommended in tutorials

The above methods were found in the analysed tutorials. All such laundering methods are in place to make it harder for issuers, banks and law enforcement to trace the money from the cardholder to the carder. They are thus used to make the transactions seem normal and legitimate. Therefore, it is stressed in several tutorials to use middlemen accounts and gateways as they can contribute to this perceived normality of transactions.

Once carders have obtained stolen card details, they will try to send funds from the cardholder to oneself and try to obfuscate the money stream and/or make it appear legitimate. In the visualisation below, in Figure .2, an example of how a fraudster could send funds from stolen cards through various middlemen accounts, all owned by the carder, can be seen.

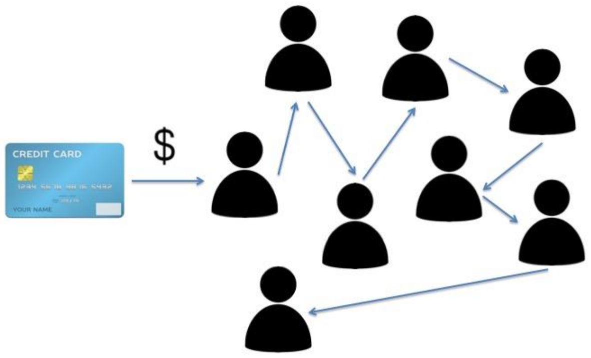


Figure 4.2 Usage of middlemen accounts by fraudsters

In Figure below it can be seen how a fraudster can use various accounts and gateways, such as payment processors, to further obfuscate illicitly obtained funds. For example, the fraudster could take the funds from stolen cards, store it at an online payment processor and from there on send it to another middlemen account to further obfuscate the trail from cardholder to carder.

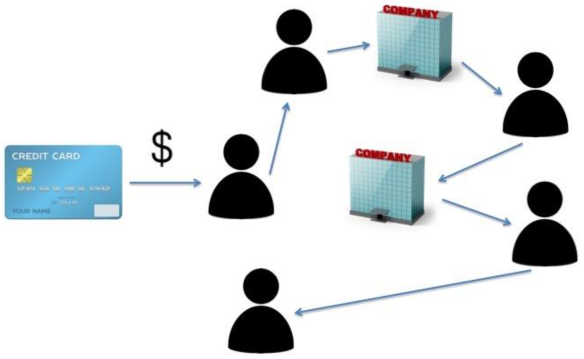


Figure 4.3 Usage of middlemen and gateways by fraudsters

Finally, to make transactions seem more legitimate and more untraceable, a carder can use several stolen cards owned by different cardholders to advertise a non-existent product on a gateway (company's website for example) and to pay the 'advertiser', whose stolen card details the fraudster will control, with another stolen card. In this way, transactions appear legitimate. The fraudster can then send the funds to his/her own account, after also advertising non-existent products. By doing this, large amounts of money can be transferred from accounts to the fraudster while raising minimal suspicion. A visualisation of this can be seen below in Figure .

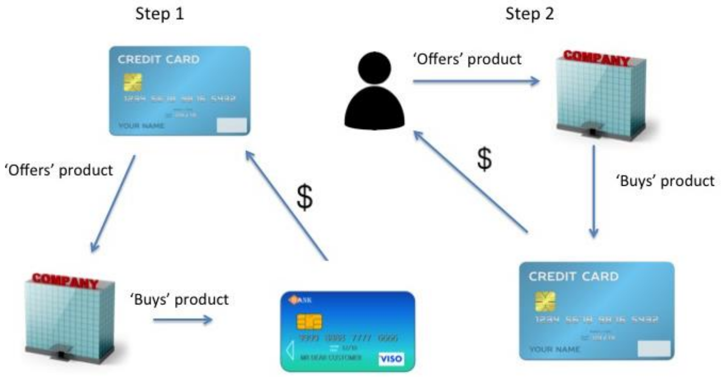


Figure 4.4 Usage of various stolen cards by fraudsters

Security steps were often also stressed in the laundering methods in tutorials. However, for clarity these were left out in Figure .2, Figure and Figure as they often overlap. For example, mostly it is recommended to use SOCKS5 to pretend to be the cardholder, as otherwise security algorithms might detect if the card is used far away from the location it is usually used from. All such steps can be seen in the *pre-entry* phase of this script analysis.

Next to the most common laundering methods, there are also methods that are mentioned less often in the tutorials. Online poker is for example one method in which stolen card details get used, as it allows the carder to play with multiple accounts linked to different cards and names and thus to cheat the game and make profits. Another method is the purchase of coins in massively multiplayer online games, such as for example Runescape or World of Warcraft, with the stolen card details and then to resell them in order to launder the dirty funds. Trend Micro (2016) has also identified the usage of games in this manner as one of the more popular methods by cybercriminals to launder illicit funds.

It must be taken into consideration that only 25 tutorials were analysed and that therefore there will thus be many other (laundering) methods. The methods that will be offered in paid tutorials, for example, may be more sophisticated and specialised, as large amounts of money is paid for them and they are often created by members of the community who sometimes have years of carding experience. Such high-priced tutorials with unique laundering methods may also only be sold to a set number of people. This will make the method harder to detect and increase chances of staying undetected for the purchasers of such tutorials.

4.1.6 Post-activity – Security and reputation afterwards

After carders have successfully transferred products to a drop or money into an account owned by them, a last couple of security steps were advised. It is generally advised in tutorials to not be too greedy.

> “After your vendor says that he has shipped, check your account/email and see the exact time and date that you received the payment. [...] Get your mind off the money. Go do something else, you have a life, don't you? Wait around 24 hours. [...] Just take attention to the small details, stay under their radar and DO NOT BE GREEDY.” [XVII]

Similarly, one should not order a new product before the first one has been shipped, according to one tutorial.

> “When you use a card to hit a website, do not hit another website using the same card until your order has shipped.” [II]

Also, it is advised that after every transaction a carder should clear browsing data, i.e. cookies, because if this is not done there is a risk that an IP address might be leaked somewhere during the process.

> [...] use this software to clear all cookies and stored files on your computer and not just your browser. You should then be able to make another account (wait up to 30 minutes-60 minutes each time you make an account)” [XVI]

Carders may also go back to the forum or marketplace where they bought the stolen card details and leave a review for the user from which they bought the card details to share their experience with the community. Thereafter, a carder might decide to take the profit and quit or start the process over again.

4.2 Situational crime prevention and displacement

Situational crime prevention is the original goal of crime script analyses. Therefore, in this section, possible SCP intervention points will be listed, after which the utility of these findings will be examined.

Structural choke points need to be identified in an online criminal environment before potential SCP measures can be put into place (Leontiadis & Hutchings, 2015). While the critical points for illicit transactions might be perfectly legal, it is still valuable to list some of them, as they might give new insights into how certain tools are abused. This can, for example, help in thinking about possible countermeasures companies that own such tools can take. Below in Table , some of the potential measures that may help in reducing the abuse of stolen payment card details are shown.

The measures are based upon sixteen opportunity-reducing techniques introduced by Clarke (1997), which can be seen in the last column. The techniques fall under the categories of ‘increasing perceived effort’, ‘increasing perceived risk’, ‘reducing anticipated rewards’ and ‘removing excuses’. The sixteen opportunity-reducing techniques identified are: *target hardening*, *access control*, *deflecting offenders*, *controlling facilitators*, *entry/exit screening*, *formal surveillance*, *surveillance by employees*, *natural surveillance*, *target removal*, *identifying property*, *reducing temptation*, *denying benefits*, *rule setting*, *stimulating conscience*, *controlling disinhibitors* and *facilitating compliance*. These are the sixteen original techniques identified by Clarke (1997). While these techniques were initially put into place for physical crime, they can also be used in an online context, as shown by Willison (2006) who used it to design opportunity-reducing techniques to decrease employee computer crime. A further nine techniques were introduced by Cornish and Clarke (2003) after critique by Wortley (2001) to complement the initial model, but these were not used in this research, as most of these points focus on the ‘reduction of provocation’, which is not applicable to stolen payment card fraud and more generally debateable, because it could lead to victim-blaming instead of dealing with underlying (societal) issues.

Scen e	Structural choke point	Potential measures	Opportunity reducing technique classification
1	Obtaining cryptocurrencies	Enforce legislations which demand cryptocurrency exchanges to know real identity of their customers	Entry/exit screening
1	Plant tutorials	Plant tutorials with false information, for example leading fraudsters to non-secure tools, on forums and marketplaces	Deflecting offenders
1	Illicit forums	Takedown illicit forums that focus on carding	Access control
2	Use of VPNs	Make agreements with providers to get access to IP addresses of users that use service for illicit purposes	Controlling facilitators/Rule setting
2	Use of SOCKS5	Make agreements with providers to get access to IP addresses of users that use service for illicit purposes	Controlling facilitators/Rule setting
3	Obtaining cards	Put pressure on companies that store card data to increase security measures, so chances of data leaks diminish	Target hardening
3	Criminal conscience	Infiltrate in criminal community and stress how severely actions affect victims	Stimulating conscience
4	Website security	Motivate smaller online retailers to increase their security measures	Target hardening
4	Usability of cards	Promote the taking up of extra security measures, such as two-factor authentication, security questions and similar initiatives	Denying benefits
5	Drops	Increase surveillance when it is clear that carder uses drop address	Surveillance by employees
5	Gateways	Motivate gateways, such as event and freelancer websites, to verify events and jobs	Deflecting offenders
6	Reviews	Law enforcement can infiltrate in illicit underground forums and leave negative reviews to scare away potential clients	Deflecting offenders

Table 4.2 Potential situational crime prevention methods

4.2.1 Effectiveness of measures

It appears from Table that there are many opportunities to reduce the abuse of stolen payment card details. Several of these SCP methods could temporarily affect the success of carders, as it may complicate their methods. However, if the above measures are not executed on a mass scale, carders can simply displace tactically or geographically (Décary-Hétu & Giommoni, 2017). The great difficulty with putting effective preventive measures in place is that carders mainly use tools, for example proxy servers, which are also widely used for legitimate purposes. Also, one nation might enforce legislation on the identities of customers of cryptocurrency exchanges, but another might not. This can lead to displacement, which is an issue commonly impeding situational crime prevention measures. Therefore, this work will not look in detail at addressing these tools in a SCP manner. Instead, it will try to map the factors that can lead to using tools in a wrong manner, which may lead to new prevention measures.

While some of the SCP measurements will have a positive effect, most will not have lasting impacts if they are not taken across sectors and borders. For example, if some companies will not adopt extra security measures in online payments, such as two-factor authentication, a perpetrator simply has to present the stolen card details and can cash it out without extra security steps. While some companies may adopt two-factor authentication, a lack of mass adoption can simply lead to displacement. This will occur as long as there are alternatives to benefit from stolen card details on other platforms.

Some of the measures will even not be completely effective if they are taken on a large scale. For example, it will be hard for law enforcement to continuously seize illicit forums, which are easily set-up again. Also, illicit hidden services on Tor are notoriously hard to address by law enforcement, as the server location is often unknown. Previously, various law enforcement agencies have cooperated to takedown hidden services by seizing these servers, such as, for example, with the takedown of Silk Road 1 and with Operation Onymous (Afilipoaie & Shortis, 2015). However, despite months of expensive international cooperation, new forums and marketplaces can easily be set-up again, which can make law enforcement's efforts appear fruitless. Still, there appears to be some value in disrupting underground marketplaces, as its users will have to start from scratch again and will have lost many contacts with which they regularly traded with on the seized marketplace. Also, such takedowns are generally combined with arrests of prominent users, which can have deterrence at its goal.

4.2.2 Deviating from the underground norms

The fact that online criminals use tools that were mainly created to promote privacy, democracy and freedom is a complex issue for law enforcement agencies. Targeting these technologies does not appear to be a (feasible) solution. However, even if such technologies are completely resilient, its users will not always be. It is assumed in crime script analysis that perpetrators optimally assess whether to engage in crime or not, according to available information, time and ability. However, because of changing tactics by law enforcement, unknown vulnerabilities in tools and behavioural inconsistencies, such decisions are complicated. Users of underground markets will also make mistakes that can lead to a failure in the obfuscation of their identity. Therefore, factors influencing such biases and contextualised decisions need to be mapped. The above crime script on carding states temporary norms, according to 25 tutorials. However, users will have different perceptions of such norms while carding as they will not all have the same backgrounds, seen the same tutorials and/or the same forum discussions. Therefore, they will deviate from the established 'optimal norms' in such tutorials in different ways. Finding common deviations amongst users could add to the above situational crime prevention measures and increase the efficiency of addressing the issue of carding.

The above analysis of tutorials with crime script analysis has given insights into some of the most commonly taken paths by carders. However, it must be noted that while there are similarities across tutorials, advice in such guides is not uniformly given. Also, (prospective) carders will most likely learn carding methods in differing manners: from tutorials as we have seen in this chapter, from other users on forum discussions and in personal chats (Yip, Shadbolt & Webber, 2013), or even through word-of-mouth in local settings (Lusthaus & Varese, 2017). A carder's background, technical ability, the settings in which 'tricks of the trade' are learned and types of cards available are some examples of factors that will influence the decision-making process of a carder and will lead to different paths taken in the process of cashing out stolen card details. These also need to be mapped. Therefore, this research will in the next chapter try to understand the decision-making of carders and how they can make mistakes by exploring their organisation and tasks in more depth.

4.2.3 Permutations

According to Cornish (1994: p. 171), the nature and development of criminal expertise depends on two factors:

- The increasing routinisation of decision making
- The continuing scope for improvisation and innovation

From this, he concludes that changes in (criminal) environments will cause scripts to evolve. Scripts are thus always a snapshot in time, as the continuous 'arms race' between law enforcement and users of illicit marketplaces will spark new innovations to ensure the strongest possible security. However, there will always be best practises, which thus allow for temporal routinisation. Such routinisation should for the online criminal, nevertheless, be complex and able to deal with uncertainty to avoid law enforcement's interference.

Cornish (1994) therefore tried to account for varieties in criminal decision-making by including the 'permutations' concept to the script approach, which allows for the coexistence of different tracks in a script. In this way, the permutator "offers a heuristic device for stimulating thinking about the range of possible, feasible, and actual procedures variations and innovations", which shows the "inherently dynamic quality of scripts" (p. 175). However, sometimes the different pathways taken by criminals are so wide-ranging that they cannot be represented in one script anymore. In one of the tutorials it was, for example, stated that there are hundreds of possible ways to cash-out stolen payment card details. This would be hard to present in a clear way. Cornish (1994), however, argued that permutations are useful when thinking about how to use situational prevention strategies and also to anticipate which kinds of displacement might occur after implementing such strategies.

Listing the various pathways that can be taken in the execution of a specific crime also has the benefit that it could clarify what types of displacement can occur. This is particularly useful when a plan is made to implement a specific situational prevention strategy (Cornish, 1994). For example, when an online criminal market is shut down by law enforcement agencies, users simply move to another similar kind of market (Hutchings & Holt, 2015). However, several law enforcement agencies have joined forces and tried to solve this problem by closing-down several marketplaces at the same time, such as in ‘Operation Onymous’[25], or by closing one marketplace down first and controlling another to which users were likely to displace[26], in ‘Operation Bayonet’. Participating law enforcement agencies wanted to cause disorientation, as many users of marketplaces would not be able any more to stay in touch with their former trading partners, and deterrence, as some members of the communities got arrested. The first strategy did not prove effective in the long term, as the operation also gathered a lot of media attention and the illicit trade eventually became much larger after the operation (Décary-Hétu & Giommoni, 2017). The latter has happened too recently to fully judge its effectiveness. However, Van Wegberg et al. (2017) concluded that law enforcement anticipated displacement and disrupted the underground community in a more effective manner. Nevertheless, these measures of enforcement and prosecution are high-cost deterrents and hard to sustain over long periods of time (Afroz et al., 2013). Operation Bayonet has shown how displacement can be anticipated by law enforcement in the online criminal realm, but its effectiveness still has to be judged for the longer term.

Ekblom and Gill (2016: p. 326) argue that simple scripts with limited “choice points and behavioural branches are easier for practitioners to address”, but that in IT security large hierarchies of branches might be necessary to describe all possible tracks. Ekblom and Gill consider obtaining information about all these possible paths as “simply” an empirical research task. If information is lacking “a less finely grained picture” could be accepted. Following this approach could, however, lead to lacking perspectives that overlook crucial elements of the criminal decision-making process. In this manner, important elements of criminal processes that need to be addressed may be overlooked. Therefore, this research will not simply present some permutations, but will look at the organisation and tasks of carding more extensively with CommonKADS models.

[25] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network
[26] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

4.3 Discussion

In this chapter, a crime script analysis of the illicit use of stolen payment card details was created from tutorials found on a cryptomarket. SCP measures were proposed based on findings in the crime script. However, it has been stressed such measures can lead to displacement or even be non-executable, as the majority of tools used by carders are legitimate privacy-enhancing technologies.

CSA can be useful in pointing out the most commonly taken paths by offenders. This is a good starting point from which the causes of crime and possible deviations from commonly taken paths can be mapped. These can be very relevant in addressing (online) crime. A wide variety of possible paths in crime commission should be considered, as there, for example, can be hundreds of alternatives to cashing out a stolen payment card. Also, addressing a wider variety of potential paths taken by online criminals can decrease options for displacement. The crime script in this chapter has thus been a good starting point to start such further analysis from in the next chapter with CommonKADS models.

Chiu, Leclerc and Townsley (2011) argued that a current problem with research using crime script analyses is that scripts often do not focus on prevention measures. While the script in this chapter has led to SCP measures, there is a risk of displacement when implementing these measures. Traditionally, crime prevention programs often lead to increases in crime rates in other geographical areas. Still, these can be caused by other factors, such as changes in the offender population and opportunity structures (Hesseling, 1994). In the online realm, this has also been observed. An example of this is increased interest and more active vendors on cryptomarkets because of media reporting after large takedowns (Ladegaard, 2017). These findings show that it is important to see what the motivations of offenders are for entering crime, as displacement may keep occurring otherwise. More focus should thus lie on offenders’ motivations when thinking of designing prevention measures.

'Administrative' forms of criminology, on which SCP and CSA are based, gained popularity in the 1980s in the United States, as pragmatic thinking and 'what works' methods became commonplace. These approaches have tried to improve the "effectiveness of police administration and management of resources, professional practice and generating expert knowledge" (McLaughlin, 2007: p. 67). McLaughlin uses the concept of problem-oriented policing by Goldstein (1979) to exemplify this shift to pragmatic policing. The problem-oriented approach tried to identify problems in a clearer fashion, breakdown the current effectiveness of responses and find alternatives to current solutions. For this, Goldstein (1979) argued, it is necessary to look closely at the spatio-temporal element of crime, the "type of people involved, and the type of people victimized" (p. 246). According to Clarke (1997), there are many similarities between problem-oriented policing and SCP, such as the action research paradigm.

According to McLaughlin (2007), evaluations of problem-oriented policing have shown that it made law enforcement agencies focus on easy problems. This can be compared with the effectiveness of SCP measures in the long term, as these might lead to displacement. From this, it should be concluded that the focus of online crime research must look further than preventive measures that only intend to alter an environment or spatio-temporal elements of crime. The first type of measures, in which environments are altered, are often impossible to execute, as cybercriminal environments are sometimes unalterable or alteration is undesirable. The latter, spatio-temporal based measures, are generally hard to apply to online environments. While the Internet can be seen as a space (O'Hara, 2004) and actions are often time-stamped, spatiality and temporality are more translucent in such contexts, particularly cybercriminal ones, and much harder to set in stone than in physical spaces because of used anonymity technologies.

Prevention measures that are more focused on the why than on the how should therefore also be considered as potentially effective measures, particularly in online environments. Left realism is an example of an approach that could inform such prevention measures. Left realism is a form of criminology which sees crime "as an endemic product of the class and patriarchal nature of advanced industrial society" (Young, 1997: p. 472). It emerged in the 1980s as a response to administrative criminological initiatives. Left realism did not accept that crime can simply be removed from society with some simple measures. The social context of crime needs to be acknowledged, which, according to left realism, is the interaction between members of a ‘square of crime’, as discussed in 2.3. In left realism, interventions need to focus on all elements of this square to be effective (Young, 1997). It can inform analyses of the entire criminal process by looking at in what social context the type of crime came into being.

To get a better grasp of paths taken by online criminals, new types of intelligence need to be considered. Carding tutorials have, in this chapter, shown to be a useful new data source for such research purposes. The crime script analysis in this chapter has shown commonly taken paths by carders. This has shown to be a useful first step in mapping the ways in which carders are recommended to operate. It has set-up this work for further analysis of how carders can deviate from such recommended norms and what factors can influence this. Therefore, in the next chapter, weaknesses in tools and possible mistakes by carders will be explored. The permutations concept is used in CSA to explore the various ways in which crimes are committed. Permutations, however, do not allow for a varied and in-depth representation of crime commission, which also includes possible unsuccessful paths. Therefore, to better account for where and how online criminals make mistakes in the criminal-decision process, different methods need to be considered. In Chapter 5, therefore, the tasks and organisation involved in carding will be explored with the CommonKADS method to add depth and context to possible paths taken by carders.

Chapter 5 Exploring the organisation and tasks involved in carding with CommonKADS

5.1 Introduction

The organisation and tasks involved in carding will be explored in this chapter with CommonKADS models. This is an extension on the crime script analysis of Chapter 4. This analysis will contribute to the understanding of the carding process by analysing why carders use certain tools, what contextual factors affect their usage, how they can be used wrongly and how they affect law enforcement agencies' investigations. The organisation involved in carding is analysed with three organisation models from the CommonKADS method. First, the *problem and opportunity worksheet* is used to map the context in which carders operate. Second, the *organisational aspects worksheet* will be used to show what the structures, agents and processes are involved in carding. The *process breakdown worksheet* shows the various tasks involved in carding and what tools are required to execute these.

Next, task models will be used to show the task structure of carding. These are based on protocol evidence, which in this case are the previously analysed tutorials. This will allow for a more in-depth analysis of the carding tasks. First, the *task analysis worksheet* will be used to present a decomposition of the various tasks involved in carding. Second, the *knowledge item worksheet* will be used to show the knowledge and competences needed for these tasks. These will show where fraudsters possibly make mistakes and how tools can complicate law enforcement agencies' investigations. Finally, the characteristics of the participants in the carding process, i.e. buyers, sellers and intermediaries, will be presented in an *agent model* in Appendix A. This will show what the goals, responsibilities and constraints are of the various actors engaged in the carding process.

5.2 Organisation models

5.2.1 Problem and opportunity worksheet

Context	Problems, opportunities and other factors
Problems and opportunities	**Problems** - Assuring quality of stolen card details - Staying anonymous throughout process - Laundering funds - Trusting the right individuals - Sending and receiving money and card details - Using tools that do not leak personal information - Judging correctness of information on forums **Opportunities** - Make large (illicit) profits from low investments - Use community to better understand illicit transaction process and find card details
Organisational context	**Vision and strategy** - Facilitate in sale of stolen payment card details - Keep user base safe and loyal to marketplace **External factors** - Availability of cards - Anti-carding efforts - Status of tools - Developments in online criminal markets **Major value drivers** - Meeting place for card details - Trusted sellers - Community
Solutions	- Card testing services - Usage of legitimate services - Cryptocurrency tumblers - Guidance on tool usage - Customer reviews - Rating systems - Escrow and multisignature transactions - Automated carding shops - Community discussions on forums

Elaboration on the problem and opportunity worksheet

One of the main problems for carders is guaranteeing the quality of stolen card details, i.e. making sure funds can be taken from the cards, and staying anonymous throughout the carding process. Forums, which are often connected to illicit marketplaces, offer large amounts of information on how to do this. This leads to another problem: what information to trust? External factors also influence the carding process. These, for example, focus on how rigorously law enforcement is trying to take illicit marketplaces down, what the perception of security and vulnerabilities in commonly used tools and markets are. However, the main external factor is the availability of cards, as there would be no online illicit trade in stolen payment cards details if none were available.

Marketplaces and forums encompass important value drivers for stolen cards. They are centralised meeting points for fraudsters in which they can discuss the trade of stolen payment cards and the security practices needed in this trade. Moreover, they are spaces on which buyers can find vendors that are trusted by the community. Mechanisms that enable trust can be seen as the solutions implemented by the carding community against the most commonly encountered problems. For example, before a vendor can obtain a verified status, an already trusted member in the community will test the offered cards (Yip, Webber & Shadbolt, 2013). With such testing services, it can be established whether funds can actually be taken from the cards. To launder funds, legitimate services or cryptocurrency tumblers (or both in conjunction) are often used. This is discussed in more detail in 4.1.5.

Other solution to the trust issue buyers encounter, are dealt with through customer reviews, rating systems, centralised escrow and decentralised multisignature escrow. These were discussed in 1.2.3. Some marketplaces have even adopted automated carding shops, which make contact between buyer and seller unnecessary, as stolen payment details can automatically be sent after payment (Europol, 2017). As previously discussed, socio, technical and socio-technical trust are crucial elements in making anonymous transactions possible. All the discussed solutions above contribute to the perception of the buyer that the transaction will be successful and will therefore be safer than buying from places on the Web where such mechanisms are not in place. The solutions mentioned in the *problems and opportunities worksheet* complicate the investigatory process for law enforcement or other ‘attackers’ of the carding community, but do not make it impossible to disrupt the illicit trade. Therefore, the tasks involved in carding will be further explored in 5.3, which will show possible weaknesses in carders’ processes.

5.2.2 Organisational aspects worksheet

Organisational aspects	Variant aspects
Structure	See Figure .
Process	See Figure .
People	See Figure .
Resources	**Technology** Forums, card data, Tor, Socks5, VPN, (encrypted) messaging tools, cryptocurrencies, VMs, virtual encrypted disks, mac spoofing, RDP, VPS, amongst others. **Physical** Postal system, drop addresses.
Knowledge	- Forum rules - Security practices - Carding practices
Culture & Power	- Hierarchical structure - Carders' argot - 'Front-end' vs. 'back-end' communication

Elaboration on the organisational aspects worksheet

The diagram by Yip, Webber and Shadbolt (2013) in Figure 5.1 shows that there is a pyramid-shaped hierarchy on carding forums, similar to legitimate businesses. The social structures within carding communities thus resemble formal organisations' hierarchies. With the different roles in carding communities come different responsibilities and status. However, it should be noted that a certain status does not limit a member to certain functional roles. The *Agent model* (see Appendix A) further elaborates on this. This structure tries to establish a trustworthy environment, in which carders know whose opinions to value and who to do business with, because of their experience and status.

The process as seen in Figure 5.2 shows a formalised representation of the crime script in Chapter 4. The concurrency in the beginning of the process indicates that a buyer of stolen payment card details needs to think about security measures throughout the entire process. The steps in the UML activity diagram are further detailed in the *process breakdown worksheet* in 5.2.3. Resources used in the process of cashing out stolen payment cards are mainly technical tools that focus on keeping the carder as anonymous as possible. Resources such as forums and messaging tools focus on establishing contact between buyers and sellers of stolen card details to facilitate their trade. Other resources focus on the actual process of paying the seller of stolen card details and getting goods, bought with stolen card details, delivered.

Knowledge will mainly be obtained through forum posts, tutorials and private chats to get a better understanding of forum rules and security and carding practices. It must be noted that it is hard to establish what the knowledge level of carders are. This is the case, as it not as clear how they obtain certain knowledge, to what extent they use it and whether it is detailed enough to help them in profiting from stolen cards while staying out of hands of law enforcement. However, by mapping in 5.2.3 what tools can be used in which steps of the carding process, it can be assumed that carders will need to obtain knowledge on these tools. These will then be explored in more depth with the task analyses in 5.3 to see why certain knowledge is needed and how failing to possess this can lead to bottlenecks in utilising certain tools.

Culture and power, the last aspect of the *organisational aspects worksheet*, is particularly interesting on illicit online marketplaces, as there are subcultural habits and uses of language that are important for success within the community. A user's trustworthiness is, for example, based upon one's 'appearance' within the community, which mainly revolves around argot and other signs and signals, such as lifespan of the carder on the forum (Holt, 2010; Décary-Hétu & Leppänen, 2013), as discussed in 1.2.3. Power can also, for example, be obtained by becoming a reviewed vendor. Finally, another crucial aspect of illicit forums is their culture of secrecy. Certain information that is necessary for a transaction should not appear on the 'front-end' of the forum. This basically means that any information that can lead back to an individual should be send in private encrypted messages. Members that do share personal information violate these rules and may be banned from the forums.

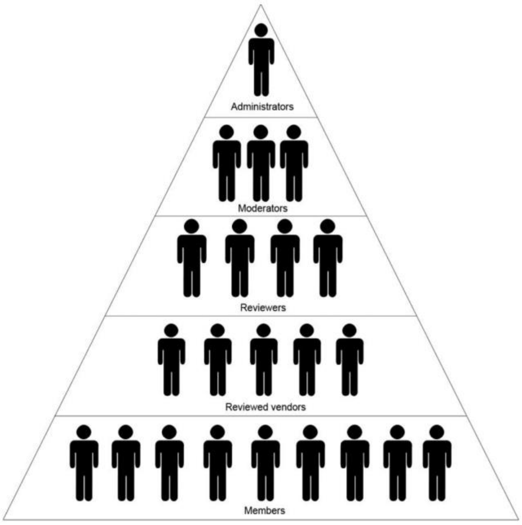


Figure 5.1 Carding forum hierarchy[27]

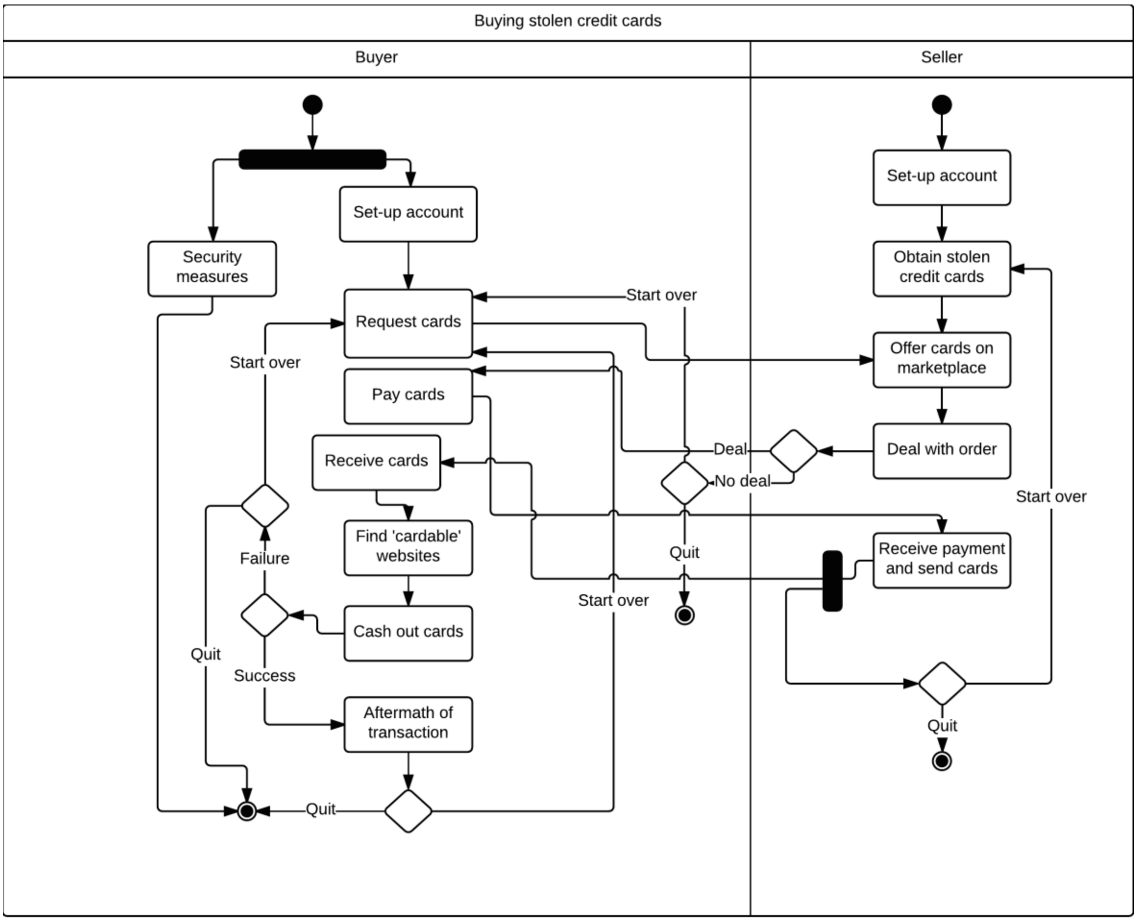


Figure 5.2 UML Activity diagram of buying stolen payment card details

[27] Taken from Yip, Webber and Shadbolt (2013)

5.2.3 Process breakdown worksheet

#	Task	Performed by	Tools	Knowledge intensive?	Significance (1-5)
1	Set-up account (preparation)	Buyer, seller	Tor, forum, cryptocurrencies	Medium	3
2	Security measures (pre-entry)	Buyer	Socks5, VPNs, (encrypted) messaging tools, cryptocurrencies, VMs, virtual encrypted disks, mac spoofing, Tor, RDP, VPS, drops	Very high	5
3	Request cards (entry)	Buyer	Forums, (encrypted) messaging tools	Medium	3
4	Offer cards on marketplace (entry)	Seller	Forums, (encrypted) messaging tools, Tor	Medium	2
5	Deal with offer (entry)	Seller	Forums, (encrypted) messaging tools	Not very	1
6	Pay cards (entry)	Buyer	Cryptocurrencies	Medium	2
7	Receive payment and send cards (entry)	Seller	Cryptocurrencies, (encrypted) messaging tools	Medium	2
8	Receive cards (entry)	Buyer	(encrypted) messaging tools	Not very	1
9	Find 'cardable' websites (pre-activity)	Buyer	Socks5, VPNs, Tor, Forum, (encrypted) messaging tools, tutorials	High	4
10	Cash-out cards (activity)	Buyer	Forums, drop address, postal service, Socks5, VPNs, cryptocurrencies	Very high	5
11	Aftermath of transaction (post-activity)	Buyer	Forums	Medium	2

Elaboration on the process breakdown worksheet

From the above *process breakdown worksheet*, it can be seen that security measures are critical and knowledge intensive. Security measures are of importance in every facet of the process of cashing out stolen payment cards. A failure to value the importance and intensity of this step could lead to a failure to obtain cards or even to an unwanted revelation of one's real identity. The task of cashing-out is the second most intensive step in the process. As this is a process of trial and error and can involve a large number of potential paths taken, it involves creative input from the carder. Whereas potential paths to cash-out stolen payment card data are recommended in tutorials and in forum discussions, carders can also think of methods themselves to profit from stolen payment card details. Such methods will either not be shared publicly or are sold on as tutorials. It is these unique methods that can be most valuable for carders, as they are not as likely to be detected by retail companies or law enforcement. Methods that occur on a more regular basis and will be executed by more people are more likely to be detected and companies can consequently put adequate countermeasures in place. The tasks described here in the *process breakdown worksheet* will be explored in more detail in the *task analysis* in 5.3.1.

5.3 Task models

5.3.1 Task analysis worksheet

The task model was created based on the crime script of carding from the last chapter and is an in-depth analysis of the individual tasks in the Process breakdown worksheet. The task model is used here to show how recommended tasks from tutorials are connected and dependent on each other in the carding process. It also looks at the goals of individual tasks and what knowledge and resources are needed to execute them. This analysis will lead into a bottleneck analysis of various tools used by carders in 5.3.2.

Task	1. Set-up account (preparation)
Organisation	This is the first step in the process of buying or selling stolen payment cards online.
Goal and value	This task is a necessary step for participation on a forum or marketplace. A pseudonymous name is the identifier of the user and communication will happen through the account.
Dependency and flow	*Input tasks*: - *Output tasks*: Request cards
Objects handled	I*nput objects*: Forum rules *Output objects*: An account, registered user name

Timing and control	This step needs to be completed before becoming active on a forum.
Agents	Buyers and sellers have to create accounts. Users who merely engage in forum discussion, but do not sell or buy also have to set-up accounts.
Knowledge and competences	Forum rules.
Resources	Forum, Tor.
Quality and performance	If the chosen user name does not exist already, the system will accept the input. Also, personal details should not be mentioned anywhere in the profile of the user.

Task	2. Security measures (pre-entry)
Organisation	The several steps in this task are important throughout the entire ‘business’ process. Users must think about this task with everything they engage in, as mistakes can alter their lives, i.e. a failure of addressing this step properly might lead to incarceration.
Goal and value	This task should ensure that one cannot lead back to a user’s real identity. Also, it should contribute to the perceived normality of transactions, which means that tools imitate regular payment patterns of the cardholder.
Dependency and flow	*Input tasks*: - *Output tasks*: -
Objects handled	*Input objects*: Security practices, carding practices. *Output objects*: -
Timing and control	The task has importance throughout the entire process. Table 5.1 shows where in the various stages of the carding process security measures can be taken.
Agents	Buyers, sellers and intermediaries.
Knowledge and competences	Proper understanding of how to use tools and services that provide users with optimal security measures. See the Knowledge item worksheet for a specification.
Resources	See Table 5.1
Quality and	If the user does not expose his or her identity and

performance	concludes an illicit transaction, this task is successful. However, this can only be said after all the tasks are completed. A carder's identity can always be exposed at a later stage too, making this the most intensive task of the carding process.

Set-up account	Request cards	Pay cards	Receive cards
- VMs - Tor - VPNs - RDP - VPS - Mac spoofing - Virtual encrypted disks	- Forums - Encrypted messaging (PGP)	- Cryptocurrencies - Mixing services	- Encrypted messaging (PGP)

Find 'cardable' websites	Cash-out cards	Aftermath of transaction
- VPNs - DNS leak checks	- SOCKS5 - Drops - DNS leak checks	- Clean cookies

Table 5.1 Security measures taken in various stages of the carding process

Task	3. Request cards (entry)
Organisation	The buyer will have to respond to an advert by a card vendor or post a request for stolen cards.
Goal and value	This task starts the process of acquiring cards for the buyer. The buyer should make a deal with the seller in this phase to obtain cards.
Dependency and flow	*Input tasks*: Set-up account, deal with offer, cash-out cards, aftermath of transaction. *Output tasks*: Offer cards on marketplace.
Objects handled	*Input objects*: Carding practices. *Output objects*: -
Timing and control	The buyer might have to go back to this stage several times, if there is a failure to strike a deal or to cash-out the cards. Also, when a deal is successful, a buyer may try to start over again and go back to this stage.
Agents	Buyers.
Knowledge and competences	Needs to be able to find trustworthy sellers on the forum and communicate with them without giving away any personal details. PGP encrypted messages

	can be used.
Resources	Forum, (encrypted) messaging services.
Quality and performance	This task will be successful if a deal is made with the seller.

Task	4. Offer cards on marketplace (entry)
Organisation	After sellers have obtained payment card details, they can advertise them on forums or marketplaces.
Goal and value	The goal of sellers who advertise stolen cards is profiting from card data, without having to cash-out.
Dependency and flow	*Input tasks*: Obtain stolen card data, request cards *Output tasks*: Deal with order
Objects handled	*Input objects*: Forum rules *Output objects*: Offered cards in forum or market
Timing and control	Sellers can offer cards on a forum as long as it is online. However, they will have to comply by the forum rules, as there can be some requirements for the offering of cards. In some cases, forums may only allow verified vendors to sell stolen card data.
Agents	Sellers.
Knowledge and competences	Needs to be able to find buyers. Before being able to advertise the cards, a seller will have to have obtained card details. A seller may have to prove quality of cards to high-up members.
Resources	Forum, (encrypted) messaging services.
Quality and performance	This task is successful if a buyer shows interest in the cards and makes an offer.

Task	5. Deal with offer (entry)
Organisation	The seller has to make a decision whether to accept the offer of the (potential) buyer.
Goal and value	The goal of making such a decision is deciding whether the price is right for the card details and whether the buyer is trustworthy, i.e. not a scammer or law enforcement.
Dependency and flow	*Input tasks*: Offer cards on marketplace *Output tasks*: Pay cards, request cards

Objects handled	*Input objects*: Offer from buyer *Output objects*: agreement or rejection of offer
Timing and control	Task is not very intensive, as the outcome is agreement, rejection or a counteroffer.
Agents	Sellers.
Knowledge and competences	Seller needs to decide price for stolen card details.
Resources	Forum, (encrypted) messaging services.
Quality and performance	This task is successful if a positive, negative or a counteroffer is given as a response.

Task	6. Pay cards (entry)
Organisation	Before receiving cards from the seller, the buyer will have to send an offer and receive an agreement for payment.
Goal and value	Sending a payment to the seller is supposed to ensure that the buyer receives the stolen card details.
Dependency and flow	I*nput tasks*: Deal with order *Output tasks*: Receive payment and send cards
Objects handled	*Input objects*: Forum rules, security practices, obtain cryptocurrencies *Output objects*: Pay cryptocurrencies
Timing and control	Every time a user wants to buy cards, a payment will have to be made. The buyer therefore needs to obtain the right cryptocurrency, generally Bitcoin, and must know into which wallet address the payment has to be made.
Agents	Buyers.
Knowledge and competences	The buyer needs to know how to obtain and use cryptocurrencies.
Resources	Forums, (encrypted) messaging services, cryptocurrencies.
Quality and performance	This task is successful once the seller has received the payment for the cards.

Task	7. Receive payment and send cards (entry)
Organisation	After receiving the payment from the buyer, the seller should send the stolen card details.
Goal and value	The goal of this task is to conclude the deal. If successful, the seller can quit or start the process over again.
Dependency and flow	*Input tasks*: Pay cards *Output tasks*: Receive cards, obtain stolen cards
Objects handled	*Input objects*: Cryptocurrencies, security practices *Output objects*: Stolen card details, forum rules
Timing and control	This task has to be executed every time a seller wants to finalise the deal with a user.
Agents	Sellers.
Knowledge and competences	The seller needs to be able to set-up an account and know how to deal with cryptocurrencies and mixers.
Resources	Cryptocurrencies, (encrypted) messaging services.
Quality and performance	This task is successful if the seller received payment and sent the card details.

Task	8. Receive card details (entry)
Organisation	If the negotiations between buyer and seller are over, the seller receives the payment and card details are sent to the buyer.
Goal and value	The goal of this task is to conclude the obtaining of stolen card details from the buyer's point of view.
Dependency and flow	*Input tasks*: Receive payments and send cards *Output tasks*: Find 'cardable' websites
Objects handled	*Input objects*: (encrypted) messaging services *Output objects*: Thinking about carding practices
Timing and control	This task occurs every time at the end of a completed deal with a seller. This preludes efforts to make profits from the stolen card details.
Agents	Buyers.
Knowledge and competences	No specific requirements for this stage.
Resources	(Encrypted) messaging services.
Quality and performance	This task is successful if the buyer receives the stolen card details.

Task	9. Find ‘cardable’ websites (pre-activity)
Organisation	This task focuses on how the buyer will try to make a profit from the stolen card details.
Goal and value	This task focuses on the planning of how to maximally profit from stolen card details. The carder will try to find the right websites that can be used with the stolen card details.
Dependency and flow	*Input tasks*: Receive cards *Output tasks*: Cash out cards
Objects handled	*Input objects*: Security practices, carding practices, forum discussions, tutorials *Output objects*: A plan of how to cash out the stolen card details, ‘gateway’ and ‘middlemen’ accounts
Timing and control	This task is intensive. It involves reading, planning and creating various accounts on different platforms. However, once the carder finds a ‘bulletproof’ method that can be used several times, this task will decrease in intensity if executed again.
Agents	Buyers.
Knowledge and competences	Carders will have to know how to be able to set their computer to the location of the cardholder, to avoid retailers picking up on deviations from regular buying patterns.
Resources	Forum, VPN, Tor, SOCKS5, (encrypted) messaging services, tutorials, stolen card details, retailer websites.
Quality and performance	This task is never fully completed, as some websites might not be ‘cardable’ anymore after a while. Therefore, the carder will have to keep looking for new methods. However, the task can be seen as successful when a ‘cardable’ website is found, as a carder is then ready for the next step.

Task	10. Cash-out cards (activity)
Organisation	As a continuation of the last step, this step represents the most important part of the carding process. In this task, the carder will try to obtain money or goods with the stolen card details or launder the money to oneself.
Goal and value	The goal of this task is to make a profit, either in money, goods, services or vouchers. The execution of this task is crucial for the success of the entire

	process. If this step fails, the carder will lose money, as the cards were obtained for a price.
Dependency and flow	*Input tasks*: Find 'cardable' websites *Output tasks*: Aftermath of transaction, request cards, quit
Objects handled	*Input objects*: Carding practices, security practices, tutorials, forum discussions, card details, information on cardholder *Output objects*: Goods, money, services, vouchers
Timing and control	This task is time-consuming. It involves a wide variety of steps, of which some can take-up a large amount of time, such as setting-up drops and laundering money.
Agents	Buyers.
Knowledge and competences	Creativity is key in this aspect of the carding process. While the carder needs to know how and when to use security measures, such as SOCKS5, VPN, Tor etc., the success of the process of obtaining goods or laundering money is determined by trying out various ecommerce platforms.
Resources	Forum, drop address, postal service, SOCKS5, VPN, Tor, cryptocurrencies, stolen card details, tutorials, retailer websites, middlemen and gateway accounts.
Quality and performance	This task is completed if a carder has obtained goods, money, vouchers or services.

Task	11. Aftermath of transaction (post-activity)
Organisation	This task is carried out after a carder has been successful in cashing-out stolen card details.
Goal and value	This task is not important for the carder to successfully make a profit from stolen card details. However, it can be important for the seller to build-up a reputation.
Dependency and flow	*Input tasks*: Cash out cards *Output tasks*: Quit, request cards
Objects handled	*Input objects*: Forum *Output objects*: Reputation
Timing and control	This task can be executed after a transaction has been completed. In that case, a buyer would leave a review to a seller and the buyer would clear cookies and make sure not to order another product from

	the same website if an order is still pending.
Agents	Buyers and sellers.
Knowledge and competences	The buyer needs to know how to leave a review and how to clear cookies.
Resources	Forum
Quality and performance	This task is completed if a carder quits or starts the carding process over again.

5.3.2 Knowledge item worksheets

This section will look into exploring how ‘knowledge items’, i.e. tools used by carders, are used. In doing so, it identifies possible bottlenecks, both for carders and investigators of such cybercrimes. In this way, it is shown how carders use these tools to complicate law enforcement’s investigations, but also where carders can make mistakes in this process. The CommonKADS method normally provides a separate worksheet per ‘knowledge item’, which are the features that are needed in performing tasks (Schreiber et al., 2000). However, in this work a worksheet is used per category of knowledge items, i.e. tools used by carders, as there is a lot of overlap within tools. The tools carders were found to use are categorised as *proxy-based services*, *cryptocurrencies* and *physical*. Within these categories the following tools will be discussed: VMs, VPNs, SOCKS proxies, Tor, RDP, mac address changers, DNS, Bitcoin and drops. These tools were selected as they were mentioned in several tutorials and because of their wider applicability across other cybercriminal domains.

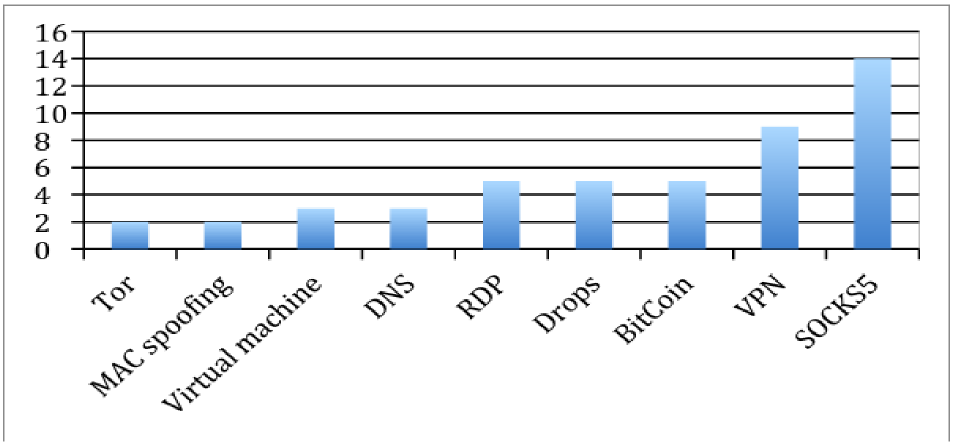


Figure 5.3 Number of mentions of tools in tutorials

5.3.2.1 Proxy-enabled services

Virtual machines

It has been recommended in three of the analysed carding tutorials to use a virtual machine (VM). VM software allows users to create multiple isolated virtual computers that run within a single physical computer. VMs can be run as part of a cloud environment, which leads to a wide variety of issues for law enforcement in their investigations (Healey, Angelopoulou & Evans, 2013). According to some of the authors of tutorials, carders should work on virtual machines to have a safe and separate place from their personal computing in which they can do their carding business which then will be very hard to trace for law enforcement. Also, by using a virtual machine for carding and the 'normal' computer for regular browsing activity, the carder is less likely to leave traces of their real identity anywhere in a carding environment or vice versa for leaving evidence behind on the physical computer. Online criminals can thus commit their crimes in the cloud while deleting evidence on their physical computer. To investigate such crimes, forensic investigation needed to adopt new techniques. These are known as cloud forensics (Zawoad & Hasan, 2013).

Cloud forensics has to deal with different issues than traditional digital forensics. Dykstra and Sherman (2011) identified the acquisition of data as one of the main issues of cloud forensics. In a cloud environment, data does not have to be stored on the physical computer of the user, but will be located on various computers owned by the cloud provider. Data and log files will be co-located with data of other users in several data centres (Healey, Angelopoulou & Evans, 2013; Zawoad & Hasan, 2013). Another acquisition problem is that law enforcement needs search warrants to access data on cloud providers' servers or to seize servers. This is problematic when the data is not located at one specific location or when the data of other users is stored on the same server, as seizing these servers can then violate their privacy. Cooperation of the cloud provider can help in such cases to figure out the best approach, as they will have, at least some, evidence of what data belongs to a suspect (Zawoad & Hasan, 2013). When using a VM on a cloud service, it acts as a proxy, as the user's actions appear to come from the VM, which is on the network of the cloud provider. Cross-jurisdictional approaches can be necessary if the data are stored at several data centres.

While using a VM on a local machine, it is also advised in one tutorial to use TrueCrypt on top. TrueCrypt is on-the-fly encryption software, which means that only the data needed by the user is accessible and that all data is encrypted from the onset (Balogun & Zhu, 2013). Furthermore, TrueCrypt can create encrypted hidden volumes on the VM and thus make it harder for law enforcement to seize data from it. In this tutorial, the argument for using TrueCrypt is made as the suspect could pull their computer's plug when law enforcement tries to enter their house. In such a case, it would become impossible to enter the hidden volume, even when the VM is decrypted, as the hidden volume will not appear to investigators. The user will have to decrypt the hidden volume before it appears. This can thus lead to plausible deniability of the suspect.

Such incidents, in which data is encrypted, are not prosecutable in sixty percent of the cases because of a lack of evidence, according to Balogun and Zhu (2013). Therefore, law enforcement often tries to prevent a suspect of an online crime from closing or turning off their machine during an arrest, as this could lead to loss of evidence. However, developers have discontinued development of TrueCrypt since mid 2014. This means that potential vulnerabilities will not be patched. However, several parties, such as the German government (German Federal Office for Information Security, 2015), have tested its code and found little risks in using TrueCrypt. However, the fact remains that new security issues will not be fixed by TrueCrypt's developers. Therefore, it may become insecure. Carders that still download TrueCrypt, as recommended in tutorials, might take a risk by using this software, as security issues may come up that will not be fixed.

The main bottleneck for doing proper investigation by law enforcement or companies into the use of VMs by carders is the limitation of access to the VM that was used by the perpetrator. This is the case because there is a strong dependence on cloud service providers in data acquisition (Zawoad & Hasan, 2013) and problems with accessing data on local VMs because of encryption (Balogun & Zhu, 2013). Furthermore, issues around space can be present, as it is sometimes unknown where data is located. If data is stored across several jurisdictions this will lead to problems, as differences in international laws can complicate the investigation process (Zawoad & Hasan, 2013).

VPNs

Virtual Private Networks (VPNs) are among the most discussed topics in the analysed carding tutorials. In some tutorials it is said that a VPN should be used at all times when a user is browsing the Web while doing something related to carding, as it helps prevent leaving a real IP address behind. Users of underground markets will sometimes even use several VPNs, proxies and the Tor browser at the same time to achieve strong security (Europol 2014). While this will obfuscate the path to a user's IP address, it will also slow down the traffic of the carder. Usability can sometimes be an important concern for carders, as it can lead to acceleration of business. It can, however, also lead to lacking operational security. Sundaresan et al. (2016), found that of merchant account on underground forums, the majority of users, 95.2%, lack in operational security by not always using a VPN. These users will thus be at risk of revealing their IP address, which could be used to deanonymise them.

The usage of VPNs will make users less prone to third party snooping on their personal IP address. However, there are still methods employed by law enforcement to identify users of these services that use it for illicit activity. Law enforcement agencies have in the past used informants to operate VPNs. They also have obtained VPN log files through court orders. Because of such developments it has been suggested that users of VPNs who use it for illicit activity are moving away from the services to Tor and botnet-enabled proxies, as they do not trust them anymore (Hutchings & Holt, 2017). This shows that an increased law enforcement focus on specific tools could lead to an uptake of technically more complex tools and even innovation. These unintended consequences are also seen in others areas of law enforcement such as sentencing policy (Webber, 2010; Grabosky, 1996).

VPN providers can be forced by law to store log files and to reveal the IP addresses of users of their service. While there are VPN providers advertising that they do not keep logs, arrests have still occurred after law enforcement seized one of their servers with a court order on which IP transfer logs were found

(Hutchings & Holt, 2017). The majority of popular VPN services[28] claim to not store log files. However, this is sometimes specified as logs of a user's browsing history, which can mean that the provider still has access to logs of timestamps, user names, payment details and so on. Most of the VPN providers log the source IP address of users when they log into the VPN. This can be a bottleneck for using a VPN for carders. However, some providers are able to circumvent laws that require logging by basing their services in countries with lenient data retention laws. This can be a bottleneck for law enforcement investigations.

SOCKS proxies

In more than half of tutorials it is recommended to use a SOCKS proxy on top of a VPN. According to one tutorial, SOCKS proxies are not as widely blacklisted by merchants as VPNs, as they are often not as publicly listed. SOCKS proxies can thus be used to access a wider variety of sites than with popular VPN services. This is a bottleneck for online merchants and investigators of cybercrime.

SOCKS proxies often run on the machines of people without their knowledge when they are part of a botnet. An attacker would install a tool on compromised machines that can open chosen ports, port 8975 for SOCKS, turning it into a SOCKS proxy (Kaspersky Lab, 2016a). A network of such compromised machines can be used for spam distribution (Göbel, Holz & Trinius, 2009). Spam server blacklists can then be circumvented (Ianelli & Hackworth, 2007), as the IP addresses of the compromised machines most likely do not appear on blacklists yet. According to Roberts et al. (2010), an issue for users of SOCKS proxies is that it is impossible to find out who runs it. They could thus be run by a government, which would allow analysis of who is using the proxy and what they are looking at. Trusting the wrong SOCKS proxy provider could thus endanger fraudsters.

RDP

[28] See http://uk.pcmag.com/software/138/guide/the-best-vpn-services-of-2017 for some examples

Remote desktop protocols (RDPs), or remote desktop connections, were mentioned in five of the analysed tutorials. RDP has a similar effect to using a proxy, making the user's activities appear to come from the address of the remote machine. RDP is recommended in one tutorial as an alternative to a SOCKS proxy, as the accessed computer can also be based in the area of the cardholder. Remote desktop connections to legitimate computing resources are offered by legitimate companies. However, remote desktop connections to hacked computers are also offered on underground marketplaces. In such a case, the owner of the computer will still have access to the computer, but carders will use their computers as proxies for carding activity.

Goncharov (2015) found that online criminals scan hacked computers for online vendor accounts (such as Amazon and eBay credentials for example), payment systems (such as PayPal) and gaming sites amongst other things. The found credentials can then be sold on underground forums and be abused for fraud purposes. Furthermore, marketplaces have sprung up, purely focusing on the purchase of hacked RDP servers. One of these marketplaces[29] offered over 70.000 hacked servers from all over the world that can be accessed with RDP, for six dollars per server (Kasperky Lab, 2016a). However, the hacked computer's IP addresses used by online criminals were later leaked (Kaspersky Lab, 2016b). This could steer law enforcement into the right direction, as they then can find out which computers connected to the compromised RDP, to identify the IP addresses of online criminals and consequently locate them. Fully trusting a RDP can thus be a behavioural mistake, as data leaks on marketplaces may lead to the apprehension of the users using RDPs for illicit online activity.

DNS leaks

It is recommended in three tutorials to do a Domain Name System (DNS) leak test, to see whether the traffic of a user of proxies or anonymity services is completely routed through the service's servers. DNS translates domain names, such as example.com, to IP addresses. ISPs will provide a DNS server for customers to use, and these servers will commonly log addresses which users have looked up. If an operating system still uses the default DNS servers ascribed to a user by an

[29] http://xdedic.biz

ISP when a proxy is in place, analysis of the DNS logs can be used to determine the browsing activity of the user. There are tools[30] available to check whether one's DNS is leaking, which were recommended in some tutorials. If a user finds out that not all of the traffic goes through the proxy, another proxy may be obtained and other DNS leaks tested, until all traffic routes through the proxy. Not doing such a test could lead to a failure in spotting wrong configurations, leading to traffic not routing through proxies and making it easier to be traced.

Mac address spoofing

MAC spoofing is mentioned in two tutorials. Media Access Control (MAC) addresses are unique identifiers assigned to devices on a network, such as a computer or smartphone. MAC addresses are often printed on the hardware of the devices (Pandey & Saini, 2012). There are, however, methods to change the MAC address in a network. This is commonly referred to as MAC spoofing (Gupta et al., 2009). Since MAC addresses are only visible to devices in the same network, they are of little use or relevance in the online world. However, devices share MAC addresses with public WiFi access points, even if they do not connect to the access point. Logs of when a MAC address was seen by a particular access point can be used to infer information such as location, but can also be correlated with CCTV to identify an individual (Minch, 2015). It is thus recommended to users in two tutorials to use tools that can spoof MAC addresses. Some anonymity-focused operating systems, such as TAILS[31], offer tools for MAC spoofing. The analysed tutorials do not specify why one would spoof a MAC address. However, failing to spoof a MAC address when using public WiFi could lead to a carder's identity becoming known.

Tor

Tor was, surprisingly, only mentioned in two of the twenty-five tutorials. However, the tutorials were all distributed on a hidden service on Tor[32], which implies that carders who accessed the tutorials in this way were already using the network.

[30] For example, https://www.dnsleaktest.com/

[31] https://tails.boum.org

[32] With the exception of applications such as Tor2Web (https://tor2web.org), which makes hidden services, i.e. sites with a .onion prefix, available through regular Web browsers

Research has shown that almost sixty percent of known hidden services focus on the trade in drugs and weapons, counterfeit products, stolen credit cards and otherwise hacked accounts (Spitters, Verbruggen & van Staalduinen, 2014). There is, however, an issue with such findings as hidden services can focus on several (criminal) domains at the same time. Other research has therefore argued that hidden services on the Tor network are most commonly used for criminal activity (Moore & Rid, 2016). More niche crime areas on hidden services range from illegal wildlife trafficking (INTERPOL, 2017) to mobile malware (Kaspersky Lab & INTERPOL, 2017). Because of the increased anonymity Tor offers over regular Web browsing, it has become a popular and indispensable tool for online criminals.

Despite the anonymity characteristics of Tor, various researchers and law enforcement agencies have managed to deanonymise users. Lewman (2016) has argued that this is possible, because hidden service are single machines connected to the Internet and that there will thus still be opportunities for investigative and technical approaches to deanonymise traffic and users. Biryukov, Pustogarov and Weinmann (2013) have, for example, shown that an attacker can correlate IP addresses to hidden services after taking over one or more guard nodes, which are extra nodes in the Tor network that the hidden service trusts and selects for users to reach its service through. They were introduced to stop attackers from finding out the IP address, as the attacker would then never own the node next to hidden service (Øverlier & Syverson, 2006), but with the method of Biryukov, Pustogarov and Weinmann the attacker takes over exactly that node. Researchers and law enforcement have exploited other vulnerabilities on Tor. An interesting example of this is when the FBI subpoenaed Carnegie Mellon University researchers for information that could lead to the IP address of a hidden service user they were investigating[33].

Tor is not the only available anonymisation service. Freenet and i2p have also been available for many years, but not enjoyed the same popularity as Tor. Distributed marketplaces are also being developed[34], complicating takedowns and identifying illicit from a technical point of view. Vulnerabilities in Tor have been

[33] https://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds

[34] For example, OpenBazaar

used by law enforcement, for example, for the identification and subsequent arrests of hidden service users who enabled JavaScript in their Tor browser[35]. Some websites will not work without JavaScript enabled, but it thus also has been exploited to uncover users' IP addresses. This is again a trade-off between usability and security.

5.3.2.2 Bottlenecks of proxy-enabled services

Nature of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Formal, rigorous	x		x
Empirical, quantitative			
Heuristic, rules of thumb			
Highly specialised, domain-specific			
Experience-based			
Action-based			
Incomplete			
Uncertain, may be incorrect	x	x	
Quickly changing			
Hard to verify	x	x	

Form of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Mind			
Paper			
Electronic	x	x	
Action skill			
Other			

Availability of knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Limitations in time			
Limitations in space			x
Limitations in access	x	x	
Limitations in quality	x	x	

[35] https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting

Limitations in form

The previously discussed *proxy-enabled* services are ‘formal and rigorous’. This means that they are based on formal technical mechanisms that strengthen users’ online privacy. As these tools are intended to protect people’s privacy, they will be used for legitimate and illicit reasons. That is why technologies such as Tor are often described as a double-edged sword (Chertoff, 2017; Jardine, 2015). However, this makes it harder for law enforcement to deal with illicit users of such anonymisation or privacy-enhancing technologies, as a part of their goal is to make it impossible for third parties to find out the identity of users and their browsing activity. Space is another bottleneck for traditionally territorial law enforcement agencies in investigations, as proxies make it harder for them to pin down the location of an online offender, who can make it easily appear as if their Internet traffic is coming from various locations. International cooperation and cross-jurisdictional approaches are necessary in addressing online crimes, making investigations more complex and costly when compared to traditional (street) crime.

Being certain about the proper workings, i.e. the quality, of *proxy-enabled services* is a potential bottleneck in the operations of carders. This is the case as the quality of tools can be uncertain and hard to verify. For example, an illicit user may not know whether a law enforcement agency is cooperating with a VPN provider. Also, vulnerabilities in tools can, for example, expose IP addresses of users. Carders may be aware of tools to use, but might not have access to them. This can be the case, as governments sometimes block access to proxy-enabled services or only allow access to a select number of government-approved tools, which most likely will be closely surveilled. Bottlenecks and chances of properly masking one’s identity are thus context and location-dependent. Furthermore, law enforcement agencies can exploit insecurities by, for example, using vulnerabilities in tools to deanonymise users or even by running proxies. Recommended paths in tutorials may thus not always be safe.

5.3.2.3 Cryptocurrencies

The cryptocurrency Bitcoin is mentioned in five tutorials. Carders' two main uses of Bitcoin, and other cryptocurrencies, are to pay for stolen cards and to obfuscate the money trail from cardholder to carder. Users can generate a new public-private key-pair, to generate new wallets, for every new transaction to enhance their privacy (Reid & Harrigan, 2013) or use mixers to obfuscate the money trail. Often, it is advised to sellers to launder the received money by using mixing or tumbling services, which are sometimes even built-in in cryptomarkets (Cox, 2016). Users can send their cryptocurrencies to such a "pool of funds and then receive them back (minus a small commission) into newly generated 'clean' addresses, thereby breaking the financial trail" (Europol, 2014: p. 42). As long as the mixing service does keep the information of whose coins it mixed private, it will be basically impossible for an external observer to find out the identities of people behind addresses (Moser, Böhme, & Breuker, 2013). This complicates investigations into cryptocurrency funds. However, the danger of sending bitcoins to mixers for carders is that there is a chance that the service is a scam, which means they could lose all the coins they have sent.

Bitcoin uses public-key cryptography. A Bitcoin address is a hash of a public key. This address is the identifier of a wallet, which can be seen as the pseudonym of a user. The private keys are required to authorise Bitcoin transactions and are stored in a wallet file. A wallet file can hold the private keys for many different addresses, which a user can have an infinite amount of. While they can use these to transfer their bitcoins from one to the other to obfuscate the money trail and create stronger privacy, network analysis can still infer information about the path, as it is all logged in the blockchain (UK Government Office for Science, 2016).

Associating bitcoin addresses with real life identities is, however, challenging. Still, many researchers have explored possibilities of tracing Bitcoins across users. Tools such as BitIodine (Spagnuolo, Maggi & Zanero, 2014) and BitCluster (Décary-Hétu & Lavoie, 2018) analyse the blockchain to group Bitcoin transactions together that are seemingly related to find the origins of payments. Biryukov, Khovratovich and Pustogarov (2014) have shown that with an attack a significant fraction of Bitcoin users can be deanonymised, as user's pseudonyms can be linked to their IP addresses. Reid and Harrigan (2013) suggest that a user directory can be partly built by associating Bitcoin users and their public keys with offline information. Stores that accept bitcoins may store identifying information on users, such as e-mail addresses, bank account details, IP addresses and so on.

This is even more so the case with cryptocurrency exchanges. Most users acquire bitcoins through exchanges with bank transfers. Also for converting bitcoins back to traditional currencies, exchanges are used. However, using exchanges can lead to operational risks (Hayashi, Moore & Sullivan, 2015). In 2013, Moore and Christin found that approximately 45% of exchanges close down, often after a security breach in which bitcoins are stolen by hackers. While this number will be lower in 2018, as the market has matured, there is still often no guarantee that users of exchanges get their money back after breaches. The fact that law enforcement agencies can subpoena exchanges, in combination with researchers' ability to the tracking of bitcoins, makes cryptocurrency exhanges an unappealing option for large scale money laundering, according to Meiklejohn et al. (2013). Still, laundering stolen payment card details to Bitcoin or alternative cryptocurrencies is recommended in some carding tutorials, as these can be bought with the cardholder's identity, making identification at the exchange of the carder impossible. It must be noted here that they cannot be bought directly with credit cards, as cryptocurrencies are non-reversible. Therefore, carders will have to use middlemen accounts and gateways for credit cards. Exchanges can also be avoided altogether by using services that connect people willing to trade cryptocurrencies in person and exchange it for cash[36].

5.3.2.4 Bottlenecks of cryptocurrencies

Nature of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Formal, rigorous	x		x
Empirical, quantitative	x	x	
Heuristic, rules of thumb			
Highly specialised, domain-specific	x	x	x
Experience-based			

[36] Such as LocalBitcoins and LocalMonero

Action-based			
Incomplete			
Uncertain, may be incorrect			
Quickly changing	x		x
Hard to verify			

Form of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Mind			
Paper			
Electronic	x	x	
Action skill			
Other			

Availability of knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Limitations in time			
Limitations in space			
Limitations in access	x	x	
Limitations in quality			
Limitations in form			

The bottlenecks for using Bitcoin for illicit purposes focus largely on the fact that Bitcoin transactions can be tracked through the blockchain and on users' dependency on exchanges. Bitcoins can be tracked through the blockchain, which is an 'empirical and quantitative' bottleneck for carders. However, the 'formal and rigorous' elements of the technologies behind the cryptocurrency, public-key cryptography amongst others, allow for the usage of pseudonymous wallet addresses, instead of real names, and complicate deanonymisation efforts for law enforcement. The highly specialised knowledge involved in obtaining and spending bitcoins in a secure fashion can be seen as a bottleneck for both carders and law enforcement. Carders need to understand the technical mechanisms underlying Bitcoin to make sure they do not give away information leading to their identity. Law enforcement officers also need to understand the technical mechanisms underlying Bitcoin to understand what to look at when trying to lead back to the real identity of a suspect. The fact that bitcoins can change hands very quickly and sent across an infinite amount of wallets and mixed with other users' coins, is a bottleneck in investigations.

Bitcoin mixers can thus complicate blockchain analysis, but using them leads to an increased risk, as the mixing service may not return the coins sent to them (Böhme et al., 2015). Also, it is not necessarily the case that the mixing service actually obfuscates the bitcoins sufficiently, as it might not have enough customers to mix properly (Meiklejohn et al., 2013). Using mixing services that work properly is thus an issue for carders. Furthermore, the existence of pseudonymous accounts allow some regulations to be imposed on exchanges (Moser, Böhme & Breuker, 2013), which can help law enforcement agencies detect illicit users. Exchanges, which as centralised entities hold personal information on their customers, are thus a possible bottleneck for carders. For law enforcement agencies, bitcoins are harder to trace than regular bank payments. While transactions are stored in the blockchain, they are registered to pseudonymous accounts that cannot easily be linked to real identities. Also, mixing services may complicate blockchain analysis. While complex, the several potential bottlenecks in Bitcoin can give law enforcement some avenues to explore in investigations.

5.3.2.5 Physical

Drops are mentioned in five tutorials. Carders use drops for extra security when they want to obtain physical goods with stolen card details. This shows that there is an important offline element to cybercrime, which sometimes can even be local if offenders work together in the same areas (Lusthaus & Varese, 2017) or meet offline (Leukfeldt, Kleemans & Stol, 2017). It is often stressed in carding tutorials that a drop address cannot have any links to the carder’s life. In some, it is even recommended to set-up schemes in which packet mules are hired to pick-up packages from the drop and deliver to the carder’s real address. These methods are applied, as it will then be harder for law enforcement to trace packages to the carder. Carders do not only ship illegally obtained products to their homes. Hutchings and Holt (2016) also found that plastics, which are empty cards on which stolen data can be loaded to then be used in stores and at ATMs, are sent by post. The drug trade on Tor is even more dependent on drop addresses and the postal system than carding, as it cannot be dealt with purely digitally. As drugs are often sent internationally, they have to go through customs, where sniffer dogs may detect drugs and odd-shaped packages are checked. Traditional post is therefore mimicked and special concealment techniques are used to minimise chances of detection (Van Hout & Bingham, 2013).

To deliver products to a drop, a buyer and a seller need to exchange personal information, such as an address, in a message. These messages are often encrypted with PGP. Some marketplaces have started to automatically encrypt all messages of users so that sensitive information is never sent accidentally unencrypted to others. Law enforcement agencies have, however, in previous undercover operations managed to 'turn off' PGP on marketplaces. Consequently, they were able to find delivery addresses of buyers' drops or homes.

5.3.2.6 Physical bottlenecks

Nature of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Formal, rigorous			
Empirical, quantitative			
Heuristic, rules of thumb	x	x	
Highly specialised, domain-specific			
Experience-based			
Action-based	x	x	
Incomplete			
Uncertain, may be incorrect	x	x	
Quickly changing			
Hard to verify			

Form of the knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Mind			
Paper			
Electronic			
Action skill	x	x	
Other			

Availability of knowledge	Bottleneck?	Bottleneck for carders	Bottleneck for law enforcement
Limitations in time	x	x	
Limitations in space	x	x	

Limitations in access	x	x	x
Limitations in quality	x	x	
Limitations in form			

Using postal services for the delivery of illicit or illicitly obtained goods creates a risk for carders and other cybercriminals. Laziness and complacency might lead sellers to, for example, not properly conceal products, such as drugs (Martin, 2014). Similar issues exist around the usage of drops, as these can be seen as an extra unnecessary hassle for buyers. Even if a drop is used, police surveillance could be in place at the drop, if it lies in their jurisdiction. Therefore, there are many bottlenecks in this part of the process that can lead to interception of illicit goods and the real identity of the buyer.

The problem with empty houses is that activity around these can cause suspicion in a neighbourhood. Places with access to postal boxes are also risky, as they may employ CCTV. Therefore, it is hard to know whether drops are trustworthy and they may be hard to find and access. Furthermore, drops can only be used for a limited amount of time, as suspicion around them is easily aroused. Being completely sure about the safety of use of the drop is almost impossible, which makes using them a ‘heuristic’ and ‘action-based’ approach. Carders also have to deal with the uncertainty that whomever they send information and do business with, such as sellers and packet mules, may not be trustworthy.

5.4 Discussion

The CommonKADS method has been used in this chapter to explore the organisation and tasks involved in carding. It has been shown why and how carders use certain tools. Also, the possible bottlenecks which carders may encounter while using these tools and how they affect investigations into carding were presented.

The *problem and opportunity worksheet* was used to list the main problems carders face and what solutions are employed to deal with these. Also, it looked at the overall goal of their marketplaces and forums. It showed what factors affect individual carders' success. Whereas most 'solutions' are relatively easily implemented, the prolonged security of carding communities depends on contextual factors as well. Therefore, these solutions are not permanent and need to be continuously updated, depending on technological developments and policing efforts. The *organisational aspects worksheet* provided insights into the processes carders go through and what resources and types of knowledge they need for this. It also listed what agents are present in these environments, whose behaviour is further specified in the Agent model (see Appendix A). Some insights into the subcultural traits of carders are also presented. In the *process breakdown worksheet* it was shown what tasks are executed by which agents, what tools they need in the process, and how intensive these tasks are.

The *task analysis worksheet* has zoomed in on the different tasks in the carding process. The model allowed for the description of where, why and how every step fits into the carding process. This is similar to the CSA analysis of Chapter 4, but more in-depth, as it also shows what knowledge and competences are required per step and describes when tasks are considered successful. This information was used and further dissected in the *knowledge item worksheet*, where it was explored what the bottlenecks in certain tools are for carders on the one hand and in investigations on the other. It can be concluded from this analysis that there are various overlapping behavioural and technical bottlenecks in tools and their usage that can lead back to the real identities of carders.

Overall, the analysis of the organisation and tasks of carders' activities with the CommonKADS method has enhanced the crime script analysis of Chapter 4. The worksheets have added depth and context into the understanding of carders' tool usage. The task models have shown how carders use tools and where potential bottlenecks in their processes lie. These bottlenecks have shown that many factors can influence the decision-making of carders and have shown that the theories mentioned in Chapter 2 are relevant in the analysis of online criminal decision-making. These will be further explored in the next chapter. It was also discussed how the usage of these tools by carders can complicate investigations by law enforcement agencies. Chapter 6 will continue looking at the tasks involved in carding, but will do so from the perspective of expert interviewees.

Chapter 6 Expert interviews: the behaviour of carders

6.1 Interviewee classification

A thematic analysis of 19 expert interviews is presented in the next two chapters. The interviewees are classified based on the stakeholder roles in online CNP fraud, which are presented in Table 1.2 in Chapter 1. The majority of interviewees, fourteen, are working for national/international law enforcement agencies or other governmental agencies that can be seen as *public protectors*. Six interviewees are based at an international law enforcement or governmental organisation. Four of these interviewees are based at INTERPOL, one at EUROPOL and one interviewee preferred to remain anonymous and not to disclose his organisation. They make up the first group of interviewees: *international law enforcement and government*. The next eight interviewees work for Dutch law enforcement or government. Interviewees were working for teams specifically focusing on specific online crimes: an anti-laundering unit, a financial crime team and one interviewee worked as a researcher for the Ministry of Security and Justice. Together, they make up the second group of interviewees: *Dutch law enforcement or government*. The remaining five interviewees, group three, work in the *Dutch financial sector*. Four of them are both *infrastructure providers* and *primary victims* as their companies, banks and a credit card issuer, issue cards, but also suffer financially from payment card fraud. One of the interviewees works for a payment service provider and can thus be classified as an *infrastructure provider*.

Interviewee classification	Group 1: International LE	Group 2: Dutch LE and government	Group 3: Dutch financial sector
Public protector	6	8	-
Infrastructure provider and primary victim	-	-	4
Infrastructure provider	-	-	1

Table 6.1 Interviewee classification

As this research has focused on the modus operandi of carders, *public protectors* were mainly used as interviewees, as they are experienced in analysing these in order to apprehend criminals. *Infrastructure providers* mainly focus on their primary task, which is the delivery of services rather than analysing how their services can be abused. *Private protectors* will have at their core goal to minimise harm for their customers, but this does not necessarily include the analysis of modus operandi of individual users, as solutions can be implemented based on larger trends of a payment culture. For example, if a nation's legislation prescribes the usage of EMV cards, card issuers will have to oblige such legislation. If a customer is protected, the private company will generally consider its task as accomplished, whereas public protectors often still need to think about apprehension and prosecution, which is where modus operandi come into play, as these need to be analysed to find traces that could lead back to the offender.

For this research only employees from banks and a credit card company were interviewed as *primary victims*, as they have an incentive to reduce payment card fraud beyond financial motivations. This is the case, as large amounts of fraud can lead to diminished customer trust in their services (Anderson et al., 2012). Therefore, banks and credit card issuers may cooperate with law enforcement, for example in public-private alliances. Such cooperation can strengthen intelligence gathering, detection, prosecution and intervention (Dutch Banking Association, 2017). Interviewing other *primary victims*, such as individual victims and online merchants, was considered, but discarded. Individual victims will likely have no insights into the modus operandi of online criminals. Online merchants will not have as good of an oversight as banks on transaction histories and on which cards are fraudulent (Sheng et al., 2009). Also, their main priority is selling goods and services in often quite specific fields, which makes it hard to find interviewees which can be seen as representative for all online merchants. Finally, interviews with carders were considered as an option. However, the issue of access to sufficient numbers of interviewees was seen as a too serious impediment to overcome. Several interviewees at a law enforcement agency, who I was relying on to find such participants, confirmed to me that it was difficult to find such cooperating participants, even for their own research.

Fourteen out of nineteen interviewees are Dutch. The relevance of interviewing Dutch experts as the main group for this research was apparent, because of the relatively low amount of fraud in the Netherlands. This can be ascribed to its payment culture, which is, for example, visible in numbers of online banking fraud. Online banking fraud occurs when an online criminal accesses the victim's bank account and transfers funds from that account. According to the Dutch Banking Association (2017), in the first half of 2016 amounted to €148.000. Over the whole year of 2015, this number was €3.7 million. In 2011 online banking fraud was still more than €35 million (Dutch Banking Association, 2017). It thus appears that in recent years the Netherlands managed to significantly reduce online criminals' profitability from online banking fraud. In comparison to, for example, the United Kingdom, the Netherlands' online banking fraud numbers are very low. In 2016, the estimates regarding online banking fraud for the UK amounted to £101.8 million (Financial Fraud Action UK, 2017). In 2015, this was £133.5 million (Financial Fraud Action UK, 2016).

Many parties in the payment chain in the Netherlands are voluntarily cooperating to prevent fraud and to strengthen security in the payment system. This partnership has been labelled unique in Europe (Doeland, 2017). This was another reason to talk to Dutch interviewees. Also, the amount of credit card payments in the Netherlands is low, only 0.5% of total payments. This amounted to thirty million payments in 2016, worth 3 billion euros (De Nederlandsche Bank & Betaalvereniging Nederland, 2017). In comparison, in the UK, for example, credit cards were used to make 2.7 billion purchases worth £154 billion (The UKCARDS Association, 2017). Payments made with iDEAL far surpass credit card payments on the Web in the Netherlands.

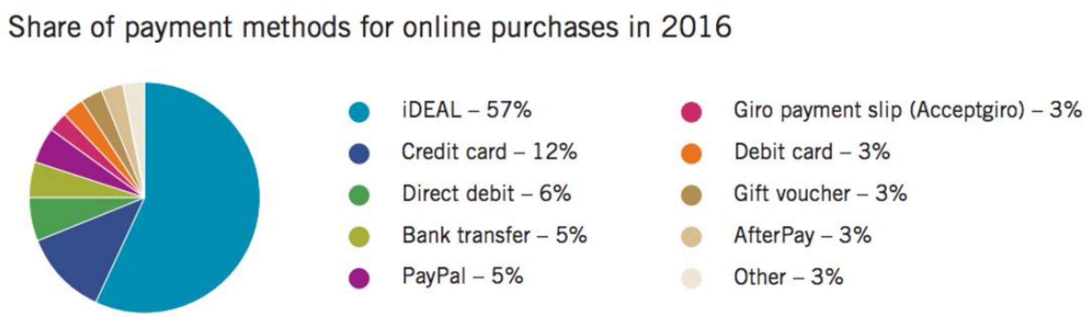
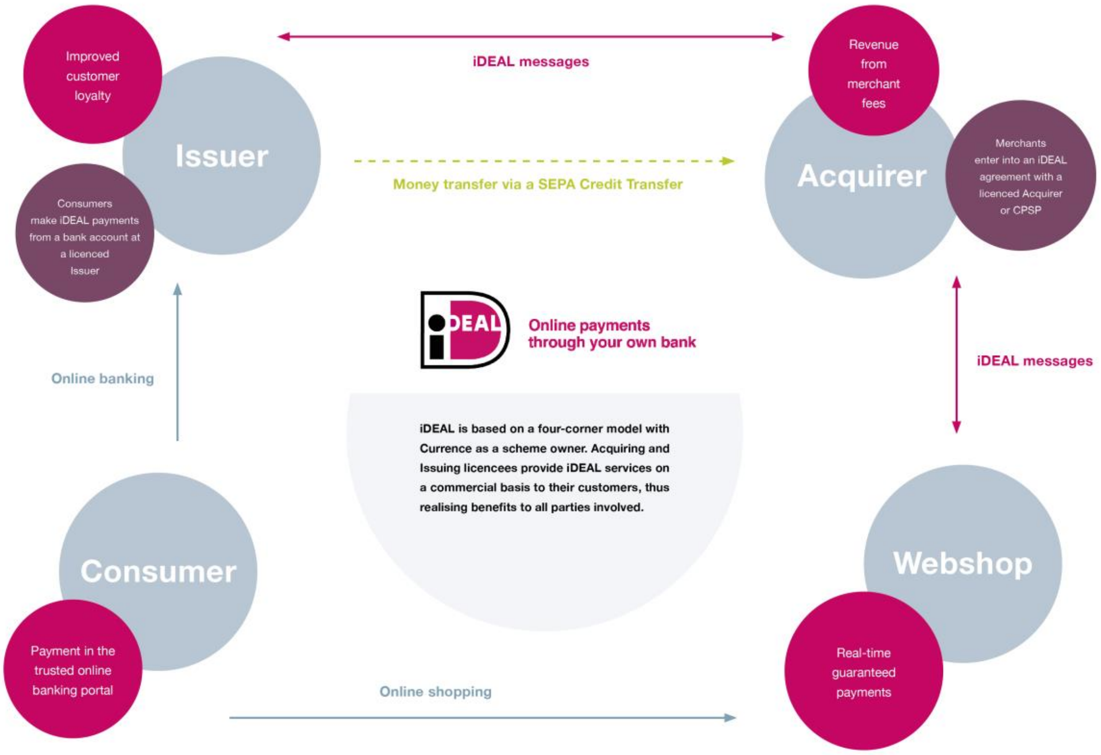


Figure 6.1 Online payments in the Netherlands in 2016[37]

iDEAL is a payment system implemented by all major banks in the Netherlands, having a reach of over 90% of Dutch individuals. Also, in 2015, over 100.000 merchants offered iDEAL as a payment method (Paypers, 2016). iDEAL is based on a four-corner model, which can be seen in the graphic below.


Improved customer loyalty
Issuer
Consumers make iDEAL payments from a bank account at a licenced Issuer
iDEAL messages
Money transfer via a SEPA Credit Transfer
Revenue from merchant fees
Acquirer
Merchants enter into an iDEAL agreement with a licenced Acquirer or CPSP
iDEAL
Online payments through your own bank
Online banking
iDEAL messages
Consumer
Payment in the trusted online banking portal
Online shopping
Webshop
Real-time guaranteed payments

iDEAL is based on a four-corner model with Currence as a scheme owner. Acquiring and Issuing licencees provide iDEAL services on a commercial basis to their customers, thus realising benefits to all parties involved.

Figure 6.2 Explanation of iDEAL[38]

[37] Taken from Dutch Banking Association & Dutch Payments Association, 2017

[38] https://www.ideal.nl/en/ideal-information/

It can be seen from Figure that iDEAL payments benefit consumers, issuers, acquirers and web shops. Consumers log-in on a trusted environment, issuers have more transactions, acquirers receive more fees and web shops are guaranteed payments and receive real-time confirmations of transactions. Consumers log-in on their trusted banking environment and will often still have to confirm a transaction with a two-factor authentication method, such as TAN-codes, QR codes, security tokens etc. It can be presumed that this leads to a relatively safe payment environment. The low number of CNP fraud is, however, the most prevalent example of the success of the Netherlands in reducing fraud and a motivation to interview Dutch experts. The absolute number of CNP fraud in the Netherlands is almost 250 times smaller than in the UK. This number can be partly explained because of the differences in payment culture and population, i.e. Dutch people almost spent more than fifty times less with their credit cards[39] than the British and also have almost four times less inhabitants[40]. The difference between the two nations is much smaller when it is normalised by credit card usage. However, the percentage of CNP fraud when compared to the total value of payments by credit card is almost five times smaller in the Netherlands than in the UK. Still, research into cultural payment habits is needed to fully explain the difference between these two nations.

CNP fraud 2016	Netherlands	United Kingdom
Total	€1.750.000[41]	£432.800.000[42]
Total value of credit card payments	€3.000.000.000[43]	£154.000.000.000[44]
CNP fraud percentage of total transactions	0.05833%	0.28104%

Table 6.2 CNP fraud in the Netherlands and the United Kingdom

[39] The Dutch spent 3 billion euros, while the British spent 154 billion pounds in 2016
[40] In July 2017 the Netherlands had just over 17 million inhabitants, while the United Kingdom had a population of over 65 million
[41] Obtained from personal communication with the Dutch Banking Association in July 2017, as official statistics were not available
[42] Financial Fraud Action UK, 2017
[43] De Nederlandsche Bank & Betaalvereniging Nederland, 2017
[44] The UKCards Association, 2017

In addition to Dutch experts, five interviewees from different countries were approached[45]. All of them work at international organisations in the law enforcement field. They were interviewed both to obtain insights into the international environment, but also to gather perspectives on a geographically diverse set of nations. All non-Dutch interviewees worked at national police agencies before moving to international organisations. It must be noted that one of the interviewees in group 1, international law enforcement and government, is Dutch. This interviewee is put in group 1, as he did work at an international law enforcement organisation. In principal, all the interviewees were asked the same set of questions[46]. During the interviews, however, the interviewee’s answers often demanded follow-up questions, making the interviews semi-structured, which is discussed in 3.3.3. While the structures of interviews were not completely the same, largely the same questions were asked. The interviewees often mentioned similar topics, which led to the possibility of using thematic analysis to analyse the interview data. From this, the following themes emerged:

- *The darknet*
- *Proxies and cryptocurrencies*
- *Mistakes and optimal paths*
- *Laundering, insider threats and the blending of the virtual and physical*
- *Security vs. convenience*
- *Impact of carding*
- *Addressing of carding*
- *Cooperation*
- *Education and public awareness*
- *Trust in technology, legislation and culture*

In this chapter, the themes with relevance to the decision-making of carders and other cybercriminals are discussed. In this way, its aim is to provide a clearer

[45] For full list of interviewees, see Appendix B. The interviewees are not ordered according to their number, this was randomised

[46] For list of interview questions, see Appendix C

understanding of the processes carders go through and to explore the external factors and cognitive biases influencing such (online) criminal decision-making. The analysed themes in this chapter are the following: *the darknet*; *proxies and cryptocurrencies*; *mistakes and optimal paths*; *laundering, insider threats and the blending of the virtual and physical*. In the next, the other themes with relevance to policing and policy-making will be discussed.

6.2 Thematic analysis of interviews

6.2.1 The darknet

As this work analysed tutorials obtained from a forum on the darknet, interviewees were asked about whether they have encountered fraudulent cards that were offered on the darknet. Several interviewees indicated that the stolen cards offered on the darknet are generally not of great quality and offered for low prices [1, 2, 12]. The estimates of how many of the offered cards still worked varied. One interviewee estimated that "80% of the card base does not work any more and maybe even 90%" [1], while another believed this number to be in between 10 and 20% [12]. The latter stressed that the rest of the cards could still be blocked, already replaced or close to their spending limit. Two interviewees from group 3 [3, 4] said that their banks do not really look at the darknet, as it is seen as too small of an issue. Contrasting views on the size of carding on the darknet were observed among two interviewees, one from group 1, who beliefs it is one of the key areas of trade on the darknet [18], and one from group 2, who sees it as a small issue [9]. According to one interviewee [11], the darknet is a hub on which stolen data is resold. It is lucrative, he argued, as cards are often sold for 20 or 30 euros each, with fraudsters sometimes selling up to 10.000 stolen cards.

Interviewees mentioned various measures that are in place to guarantee a safe community on the darknet, such as rating systems for vendors and, on a meta-level, for marketplaces[47] [8], tutorials [9], regular changing of hosting [11],

[47] Such as https://deepdotweb.com; https://dnstats.net/; https://reddit.com/r/darknetmarkets

cryptocurrencies [11], product reviews [13] and encryption [13]. Despite these measures, many marketplaces are still taken down within a short period of time, sometimes even in less than a month [10]. Still, users of the darknet are considered as being “on the sophisticated end” [17] and their usage of anonymisation services has been described as “obvious”, because of its “strong, strong anonymity” [18]. Two interviewees from group 1, however, observed an abundance of trust in technologies by online criminals. By putting their trust in online platforms, online criminals might give away too much information, which then can be used by law enforcement if they take over the platform and run it [15]. This, for example, happened in the case in which Dutch law enforcement ran a darknet marketplace for nearly a month[48]. According to [18], users of the darknet are not always cautious when communicating and engaging in transactions as they trust the technology. Consequently, he argued, they forget about basic operational security such as not mentioning personal information and habits. Law enforcement could then use such details for profiling.

6.2.2 Proxies and cryptocurrencies

The following three themes focus on the modus operandi of fraudsters engaging in online payment card fraud, with interviewees sometimes commenting on wider online crime trends. Proxies and cryptocurrencies were often mentioned by interviewees as tools used by online fraudsters to obfuscate the path leading to their real identity. It rarely happens anymore that online criminals work with static IP addresses, proxies are almost always used [2, 4]. VPNs are also used a lot [15, 18]. This leads to problems for law enforcement, as they will struggle to find the IP-addresses belonging to fraudsters [17]. However, the same interviewee stressed that many online criminals do not plan a lot around their operational security and might not even be aware “that IP address exist” [17]. Another interviewee argued that this may not always matter:

> “I have a very facetious comment: ‘you get your first cybercrime for free’. Because if you’re sitting at your computer at home, with no VPN, using

[48] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

> your own IP-address, uhm, you can commit a crime, doesn't matter what it is, if it's carding or if you're doing a hack whatever, retrospectively attributing that act to an individual, even if you got the IP-address back to a house, proving that it was a particular individual can be difficult […] Even without a proxy, [they are] unlikely to get caught the first time. With a proxy or a VPN, most unlikely." [15]

[15] also mentioned that a VPN may drop out, which can put the fraudster at risk. Furthermore, it was mentioned that using a VPN is not necessarily safer than not using one, especially when one subscribes to a service using their personal credentials [8].

Bitcoin and other cryptocurrencies are often used for criminal-to-criminal payments [13]. Traceability of these was mentioned as an issue [2], especially if cryptocurrencies end up at companies that try to anonymise payments:

> "There is not much we can do to identify the final beneficiary of the money that are paid through cryptocurrencies. […] it's still a big challenge, still not possible to trace completely, to follow the money through bitcoins, it's already difficult through credit card. If they reach some company, which are intended to anonymise the payment, which are based in some places like [mentions lots of Caribbean islands], where there is no legislation. So, even if you ask for international assistance, they won't reply, so it's difficult for the normal currencies, just imagine how it can be for bitcoins." [11]

Also, proving ownership of bitcoin wallets is hard, which might lead to difficulties in investigations [17]. However, others stressed that, while complex, all bitcoin transactions can be followed through the blockchain and thus leave more traces than cash [5, 13]. Whereas Bitcoin is sometimes referred to as an anonymous currency (Omand, 2015), two interviewees argued it is hard to get rid of all personally identifiable information links to bitcoins [5, 7]. For example, directly going from stolen credit cards to cryptocurrencies is impossible, as cryptocurrency payments are irreversible. There will thus always be something in the middle of such a chain, as credit card issuers do not accept the acquiring of cryptocurrencies, argued [5]. [7], in line with this, argued that the only way to make bitcoins unlinkable is by selling them for cash.

6.2.3 Mistakes and optimal paths

After discussing some of the tools used by fraudsters to try to stay anonymous (proxies, VPNs and cryptocurrencies), the interviewees' comments on common operational security mistakes by fraudsters were grouped together. Also, their opinions on (the possibility of) perfect operational security were grouped together. The interviewees' comments on these issues were subdivided into the categories *online*, *physical*, *behavioural,* and *money*.

6.2.3.1 Online

The fact that an online criminal only has to make a small mistake once to risk arrest, such as logging into a marketplace from their real IP address, was mentioned by [3, 8, 11]. Lacking (online) operational security, such as only using a proxy or a cryptocurrency mixer, was also mentioned by several interviewees [3, 17, 18]. A critical characteristic of online environments is that mistakes can often not be erased. Transactions on the blockchain and public forum posts were mentioned as examples of this [8, 9, 14]. This is to law enforcement's benefit, as experience on how to stay secure is only gained over time and mistakes are thus easily made in early phases of getting involved in online crime [13, 14].

> "What you often see is, this is common knowledge […] is that the mistakes are in the early stages. They may have put a Bitcoin transaction or a bank account in their own name once. You don't become a mega criminal overnight. You have to gain experience." [14]

Furthermore, online services, such as VPNs and cryptocurrency mixers, can be taken down by law enforcement, which can change optimal operational security and alter safe paths. Such developments, together with the adoption of new technologies, may be difficult to understand for online criminals and can thus lead to mistakes [8]. This shows that users do not always adopt new methods when security concerns are raised. Instead, they will often act according to their personal status quo. Other common mistakes that were mentioned are using personal credentials on retailer sites and the repetitive usage of IP addresses and drops [12, 15, 17].

> "[…] the weakest link is the person that is committing the crime, they get sloppy, they get lazy, they have a repetitive pattern of how they do things, uhm, the risks increases every time you do it. […] it's human nature […] it's difficult to come up with new drops." [15]

Layered operational security, the usage of multiple tools and money mules, was mentioned as a requirement to decrease chances of arrest [3]. To access Tor marketplaces, online criminals often use operating systems focused on anonymity, such as Tails and Whonix [8]. Furthermore, the resale of stolen data has also been mentioned by several interviewees as a quick and common way for fraudsters to quickly earn significant amounts and to try to move away suspicion to cashers [4, 11, 15]. Such stolen information is often sold on the darknet [11], on which a sophistication of vendors has occurred [13]. Some even start their own single vendor shops on .onion domains, as markets may be trusted less than successful individual vendors [8]. Technical security mechanisms to facilitate secure transactions on marketplaces have evolved. Multisignature was mentioned by [8] and [9] as an example, but [8] stressed that such services are generally not free, as there are transaction fees included. Furthermore, the usage of PGP and two-factor authentication is also something that is increasingly stimulated on marketplaces' communities and adopted more and more [8]. While marketplaces thus encourage operational security measures and more users adopt them, still not all do. This shows that users use workarounds to reach their goals and possibly suffer from status quo bias.

6.2.3.2 Physical

Stolen card details are often cashed out by ordering goods and delivering them to money mules. This was classified as risky behaviour for online fraudsters by several interviewees [1, 5, 10], with one interviewee stressing that it is difficult to find new delivery addresses [15]. Money mules are often used as a starting point in an investigation and can lead to fraudsters [19]. CCTV is another risk factor, which online criminals often do not think about. Therefore, they can get caught on camera while cashing out stolen cards at ATMs or when picking up products in shops [2, 4, 13].

> “Our most recent suspect is constantly on camera at ATMs. […] Another stupid mistake is delivering in shops, I found. They will be caught on camera there.” [2]

According to [15], staying anonymous in the physical delivery process is sometimes more difficult than staying anonymous while spending money online. One interviewee argued that vendors and buyers do not need to know each in other in real-life, but that the individuals who run shops together often do and need to trust each other [8]. This might lead to them giving away sensitive personal information, for example to an infiltrator, which could lead law enforcement to real addresses [13]. Physical products, such as anonymous post boxes and vouchers, were also mentioned by interviewees as facilitators of anonymity and have consequently complicated investigations [3, 14].

One interviewee mentioned that tutorials are updated after arrests [9]. The details of investigations often end up with lawyers and suspects, he explained. In this way, law enforcement’s “box of tricks” will become public. This can help online criminals and is a clear disadvantage for law enforcement’s efforts.

> “Criminals get arrested, their mistakes become known and, of course, those are updated in tutorials every time … so, this creates some kind of learning ability with the people who advise users” [9]

Moreover, another interviewee mentioned that during court cases involving online crime several previously convicted criminals were physically present on the public stand [14]. This will, in this context, help the viewers to decide whether to continue using certain tools in their modus operandi or to uptake a different path, depending on the reasons why the suspect was arrested and prosecuted. Two interviewees from group 1 stressed the importance of being aware of online criminals’ modus operandi and how such awareness can be obtained by questioning arrested suspects [18, 19].

6.2.3.3 Behavioural

Various mistakes made by online criminals were ascribed to behavioural characteristics. Overconfidence [13, 15, 17], inattentiveness [3, 17], laziness [8, 15], copying without understanding [8, 13] and showing off [18] were mentioned as common behavioural mistakes that can put online criminals at risk of apprehension by law enforcement. This is not surprising, as making mistakes is human, several interviewees mentioned [3, 8, 11, 13, 15, 18]. These behavioural tendencies show that users do not always make their decisions in accordance with available information. It shows that they may misinterpret available information or let their decisions be affected by intuitions, impressions and feelings. Law enforcement operations sometimes may also amplify such cognitive biases. [16] mentioned that criminals will especially make mistakes after big law enforcement operations, as they will be deterred and fiercely try to cover their tracks and will make mistakes in this process. Law enforcement anticipates commonly recurring mistakes and uses checklists to find out whether these errors have been made by a subject of an investigation [8]. For law enforcement, however, economies of scale are often at play, according to [15], as not too many resources will be spend on small players. Carders that engage in high volume and high frequency transactions are more likely to be chased by law enforcement. Still, there are no certainties for online criminals, he argued.

> “But, everywhere across that spectrum there’s a risk that you can get caught, there’s no guarantee at either end of the spectrum” [15].

Opposite views were held on the theoretical possibility of an online criminal’s perfect path of operational security. [8] believed it is possible, while [18] did not. Others argued that non-repetitiveness [1] and the usage of several user names

[13] could lead to a lower risk of getting caught. According to one interviewee [11], cybercriminals only spend 10% of their time on selling goods, whereas 90% of their time is devoted to hiding themselves.

6.2.3.4 Money

'Following the money' is a common method in the detection of suspects in online and traditional policing (Kruithof et al., 2016; Omand, 2015), but is often complicated because of tool usage by online criminals. Fraudsters will try to 'break' the online trail by using Tor and VPNs to obfuscate their IP-address, while using cryptocurrency mixers and money mules to obfuscate the source of the money, according to [3]. They also often immediately get cash at an ATM and spend it to reduce traceability. [14] argued that anonymous cards can be used by fraudsters to anonymise their transactions. Furthermore, he mentioned that if fraudsters move their illicitly obtained funds across countries and exchange it a lot, it leads to a safer position for them. Finally, he argued that stolen payment cards are often not the starting point in an investigation, but that they are used to facilitate other crimes, for which large amounts of criminal money have to be moved [14].

Two interviewees stressed that online criminals work where the money is [11, 14]. Chances of detection in certain regions may be lower, but prison time and severity may be considerably tougher, which is why online criminals also consider legal frameworks to decide from what countries they operate. Online criminals have to trust their online environment a bit and not completely "sit behind a firewall", as they otherwise cannot do business effectively, according to one interviewee [16]. Interviewee [17] similarly argued that the operational security of online criminals is thus always a battle between convenience and security. This is discussed in more detail on a policy level in Chapter 7.

6.2.4 Laundering, insider threats and the blending of the virtual and the physical

6.2.4.1 Laundering

Several interviewees mentioned the difficulties that arise when money is laundered through several countries, before it is cashed in a different country. The interviewees mentioned a wide range of hard to investigate criminal modus operandi in which the funds from stolen payment cards are laundered. Cashing through foreign debit cards [1], companies that sell vouchers in “difficult” countries [5], ATMs abroad [6] and money mules abroad [18] were all mentioned. Two prevalent topics in the context of laundering that were mentioned by many interviewees are the abuse of legitimate services and money mules.

Several interviewees mentioned the same online payment services being abused by online fraudsters. PayPal, Skrill, Neteller or WebMoney accounts are often opened with stolen ID information or by money mules. Fraudsters then order debit cards, to cash laundered funds at ATMs anywhere in Europe [1, 6, 7, 11]. One interviewee mentioned that several payment processors purposefully operate around the edge of being legitimate by having lacking security mechanisms and are therefore easily abused by online criminals [12]. A famous example of this was the centralised virtual currency Liberty Reserve, which allowed its customers to transfer without verifying their identity information. In this manner, Liberty Reserve facilitated a wide array of cybercrimes, from credit card fraud to child-abuse material to investment fraud. From 2006 to 2013, it was estimated that over six billion dollars of criminal proceeds was laundered through Liberty Reserve before it was closed down by the United States (USA v. Liberty Reserve, 2013).

Displacement to other payment systems is commonplace and easy for criminal actors, but confiscating assets from centralised entities could still be used as a deterrent by law enforcement (Thomas et al., 2015). However, when cryptocurrencies are used, it is harder to confiscate criminal assets. Because of this, and because of their pseudonymous characteristics, cryptocurrencies are often used for money laundering [5, 14, 16, 19]. Carders sometimes try to launder money by buying bitcoins and using cryptocurrency tumblers, according to one interviewee [16]. Cryptocurrency mixers are in investigations often marked as indicators for money laundering, as these are rarely used for ‘normal’ transactions [5]. Furthermore, the transferring of large amounts of cryptocurrencies is also seen an indication for money laundering [14]. Some interviewees expect online fraudsters to adopt complicated laundering methods in the future, such as cryptocurrency investment schemes[49] and investments in legitimate online services or fintech companies [5, 19].

Next to complex online laundering, more traditional physical laundering schemes are also used by online fraudsters. A common way of laundering stolen funds is by buying products [6]. Stolen card details are also used to generate plastics, which can be cashed at ATMs [14, 15]. Furthermore, stolen card details are used to buy (gift) vouchers, which can then be resold again [6, 14, 16]. Prepaid phone cards [4] and prepaid payment cards [12] are also used for laundering. According to [12] the latter’s main use in the Western market is money laundering, as he argued that there are only legitimate uses for unbanked people. Therefore, he argued, that Mastercard and Visa facilitate fraud:

> “[Mastercard and Visa] allow verification and authentication from a distance on the Internet. If I want I can easily order 10, 20, 30 prepaid cards today with your identity, then I will receive them this week, with your pin code and if I use criminal money from a Bitcoin exchanger, I can deposit it on your prepaid card. You wouldn’t notice anything, but I can then cash them everywhere on earth” [12]

Money mules are used often for online fraudsters’ laundering processes [1, 2, 6, 7, 10, 12, 16, 18, 19]. According to [10] and [12], money mules are used to protect a small network of criminals. The ‘mules’ keep them anonymous and take the risk themselves for relatively small rewards. One interviewee described the usage of money mules as the “standard modus operandi” in Europe [18]. Money mules are often recruited on the streets in poor neighbourhoods, according to several interviewees [1, 12, 16]. One interviewee also mentioned that carders use

[49] These are also known as Initial Coin Offerings (ICOs)

addicts to receive packages [1]. Leukfeldt, Kleemans and Stol (2017) concluded similarly, based on their analysis of eighteen Dutch police case files, that money mules are approached on the streets, but also at sports clubs, nightclubs and even schools. They also found an example of money mule recruitment through email. In such emails, a job was promised in which the prospective applicants only had to have a bank account in the Netherlands and forward money to new bank accounts. Interviewee [17] and [18] also brought this issue up. Criminals recruit mules with a legitimate looking job, but all they have to do is transfer money and keep a percentage for themselves. This is “money laundering as-a-service”, according to [18].

One interviewee [13] specifically mentioned that there was recently one case in which, to her surprise, no money mules were used, which exemplifies how commonplace it is. The usage of money mules also shows that social ties are often still of importance to online criminals (Leukfeldt, Lavorgna & Kleemans, 2016). Because money mules will often have been in contact with suspects, they seem like an obvious starting point in investigations. However, one interviewee questioned the usefulness of interrogating money mules:

> “There has of course been plenty of research into questioning money mules, interrogating them whatever, but the experience is that it takes up a lot of capacity and does not necessarily solve a lot. It is, however, very popular at law enforcement agencies, as it is a piece of cybercrime that everyone understands. It is just someone who you can talk to, you don’t have to do computer research or whatever, it is just someone who you can talk to and who can tell you who he is in contact with.” [7]

6.2.4.2 Insider threats

Next to money mules there are various other paid facilitators used in the cybercriminal process. These facilitators are often insiders at legitimate organisations, such as postal services or banks. [1], [2] and [16] gave various examples of postal workers being used by fraudsters to obfuscate traces leading to themselves. Mail carriers are, for example, sometimes paid to hold packages, so there is no direct trace to a house. They can also be approached on the streets by a fraudster who pretends to live on a certain address, the address on the delivered product. Fraudsters also infiltrate in the postal service. Leukfeldt, Lavorgna and Kleemans (2016) found similarly that insiders would change addresses so that postal workers could intercept mail and packages. According to one interviewee, from group 3, more and more people from criminal organisations are trying to infiltrate at banks to see how they work [1]. He sees this as a good development, as it shows that online detection is working so well, that fraudsters have the feeling they have to be part of the bank to better understand their processes to be able to defraud them. Employees who already work at financial institutions are, however, also approached by fraudsters [1] and sometimes offer to help fraudsters to launder money for a percentage of the gains [3].

Night porters in hotels were also mentioned as a group that may abuse their access to large amounts of identity documents to make illicit profits, as they can copy large amounts of bookings and resell them on the darknet [1]. Another group 3 interviewee stressed that there may be (online) merchants whose only goal is to phish customers' details, as they can then sell them on the darknet [12]. According to interviewee [6], the problem with solving such issues is that only one employee needs to be 'turned' and a fraudster can obtain a large range of identity documents.

6.2.4.3 Blending of virtual and physical

The motivation for laundering and facilitators of laundering is generally to remove traces to the criminal activity of the fraudster. The overlap of fraudsters' activity in the physical and online world was mentioned several times as being a crucial point for investigations. Online fraudsters often try to take their earnings out of the digital realm, for example, by trying to convert cryptocurrencies to fiat currency [7]. Several interviewees saw such conversion points as the most risky part of fraudsters' operations [6, 7, 12]. Both virtual and physical 'skills' are required for a successful fraudster [8, 18]. This is the case, as a fraudster, for example, needs to know how to trade and stay anonymous online, while also making sure not to get caught on CCTV while cashing or when picking up packages [9]. One interviewee [8] argued that both online criminals who originally were active on the streets and the ones that have only been active online, have advantages. The ‘digital natives’ often make mistakes on the physical front, while ‘traditional’ criminals will have more experience with this, but may, for example, make a mistake in their Tor configuration. Another interviewee mentioned that organised crime groups therefore sometimes hire young people to run online shops, also because they are increasingly seeing the darknet as an easy and anonymous way to earn more [9]. [8] further stressed the difficulty of always staying on top of this process for online criminals.

> “The digital part is only one aspect of the entire process. Maybe less so with carding … but if you sell physical goods, drugs, counterfeit money or IDs, you have to send it. Well, use gloves, pay attention you put it in different mailboxes. You can make all kinds of mistakes there. So, you have the entire digital process, the physical process and the financial process. That all has to be flawless, every day again. That’s a challenge.” [8]

According to [18], tutorials make the digital process easier for non-technical fraudsters. He also argued that the first part of the fraudster’s process is generally online, while the second is physical. Except if card details are obtained through skimming, then the whole process can be physical, he argued. [4] further argued that card fraud is a continuum which can start in the physical or in the digital and end in the physical or in the digital.

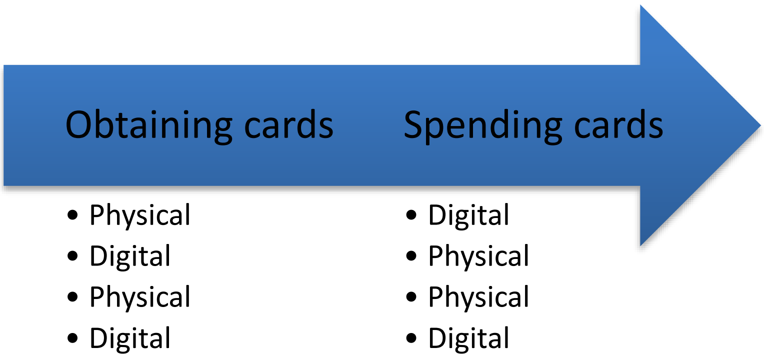


Figure 6.3 Continuum of payment card fraud[50]

[50] According to [4]

Figure shows that actors will approach risks differently, even when the same information is available to them. Also, comments by interviewees have in this chapter shown that users with different backgrounds, for example, a user with an organised crime background or a technically-educated University student, will most likely approach risks differently, as their reference points will vary.

6.3 Analysis of interviews

Several interviewees mentioned complexities in investigations because of suspects' usage of tools, such as *proxies and cryptocurrencies* or *the darknet*. In most countries such tools are legal and used for various legitimate purposes, ranging from accessing public Wi-Fi in a secure manner to accessing a corporate network to engaging in more private transactions, which are not dependent on a centralised entity, amongst others. However, several nations try to shutdown proxies and cryptocurrencies. Tor is also blocked in various countries, but this can often be circumvented with the usage of bridges or pluggable transports. These are used most by users in the United Arab Emirates, where Tor is blocked[51]. Russia, for example, has banned VPNs, anonymisation services (such as Tor) and anonymous use of messaging services, as it wants to block access to "unlawful content"[52]. China also banned several VPN services in 2017 as only services which received a license from the government are supposed to be used[53]. Reasons for blocks of proxies and VPNs may be political, such as to enhance possibilities for surveillance and inhibit citizens' anonymous browsing.

Cryptocurrency mixing services and exchanges can also be blocked or closed-down for various reasons. An exchange can be closed-down because of exit scams by its owners, hacking attacks in which large amounts of coins are stolen or if a government takes it down because of non-compliance to anti-money laundering laws[54]. Because cryptocurrencies are generally difficult to trace, some

[51] https://metrics.torproject.org/userstats-bridge-table.html
[52] http://www.bbc.co.uk/news/technology-40774315
[53] http://www.bbc.co.uk/news/technology-40772375
[54] For example, see Vinnik indictment: https://www.justice.gov/usao-ndca/press-release/file/984661/download

nation states try to impose restrictions and regulations on its use and entities dealing with them (Brito, Shadab & Castillo, 2014). Other nations have made the use and possession of cryptocurrencies illegal. While the distributed and encrypted nature of many cryptocurrencies makes tracing them harder, they are not usable on a wide scale, as they are not a widely accepted payment method. Therefore, as interviewees have stated, the conversion points from cryptocurrencies to fiat currency will remain a crucial point in investigations and a bottleneck for carders and other cybercriminals.

Interviewees mentioned that fraudsters who obtain large amounts of card data try to quickly resell it on *the darknet* to get rid of the responsibility and to make a quick buck. This is in line with comments by Holt, Smirnova and Hutchings (2016). These authors argued that when small groups of hackers steal large quantities of data they often sell it on, as they cannot use it all themselves without risking detection. However, some carders will not quickly sell, but try to learn new methods. Some of the interviewees' observations on criminal decision-making and their learning processes have exemplified this. Particularly, the comments made by Dutch interviewees about previously convicted criminals attending court cases involving cybercrime offenses are relevant here. In this way, the convicts learn about methods and mistakes made by suspects, which can be seen as their reference group.

In accordance with social learning theory, their observations serve as evaluative definitions, which is a value judgement of the suspects' behaviour, and they consequently judge it as good or bad. In other words, the suspects' past behaviour will expose the observers from the stands to "behavioural models and normative definitions" (Akers et al, 1979: p. 638). The observers learn which paths taken are likely to be punished. Consequently they can decide what new ones to continue on. Such behaviour is known as differential reinforcement (Akers, 1977). Online criminals have to be continuously aware of developments in the various tools they use. Constant learning is thus required, as failure to do so can lead to risking the possibility of exposure to law enforcement agencies.

Various interviewees further mentioned how carders and other cybercriminals abused legitimate services and money mules to launder illicit funds. The previously mentioned abuse of anonymous prepaid cards has also been considered by the European Parliament (2017), which has stated that terrorists can abuse such services in financing their attacks. Therefore, it concluded that limits should be reduced for anonymous prepaid card issuers, so that less money can be anonymously put on such cards. Money mules were also mentioned often. According to Leukfeldt and Janssen (2015), cybercriminal networks that have recruited their mules on the streets have tight control over them and will feel comfortable in sending them large amounts of money, as they often know their physical whereabouts. Mules that were recruited through "electronic means" are trusted less (p. 182), which can also be expected for the mules recruited as part of an as-a-service model, as previously discussed by interviewee [18]. Leukfeldt, Kleemans and Stol (2017) found that recruited money mules generally have debts. This shows that vulnerable communities will thus be targeted for money mule recruitment, which also explains the comments by interviewee [1] on addicts as money mules.

Large debts or serious addiction do not have to be the cause of participation in the online criminal process. The subtheme *insider threats* has shown that relative deprivation can also be a cause for participation. As insiders will receive a legitimate income, they are not necessarily demonstrably lacking something (Webber, 2007b; Runciman, 1966), which is more likely to occur in addicts or people who are in debt. Low-rank employees at banks may, for example, see their colleagues earn a much higher salary than themselves, which could lead them to being tempted to help in facilitating illicit activity, such as opening accounts for fraudsters, changing spending restrictions or leaking insider information. Insider employees act according to short-term change of wealth, earning a quick buck. However, they do not consider or fully understand their final state, which may involve arrest, being fired and legal consequences. Insiders engaging in illicit behaviour can thus be better analysed with prospect theory than models of expected utility (Farahmand & Spafford, 2013).

Mules, insiders and other contacts of carders are often met in person. Other comments by interviewees have shown that online criminality should not be approached with an overtly technological deterministic approach. The lives of online criminals drift between the online and the virtual (Webber & Yip, 2013). Some interviewees stressed that it does not even really matter how much anonymity a technology can lead to online, as a subject will, eventually, want to convert illicit gains to fiat currency or goods. Real-world usability of cryptocurrencies is not a widespread reality (yet), which means that luxury goods can seldom be bought with such hard-to-trace coins. Exchanges are therefore seen as a "vulnerable boundary" (Lewman, 2016: p. 38) and as a "chokepoint" (Meiklejohn et al., 2013: p. 135), as they enable (law enforcement's) tracing of cryptocurrencies, which consequently complicates large-scale money laundering. Furthermore, interviewees focused on the differences in strengths of types of fraudster based on their mode of entry, i.e. coming from a 'traditional' crime background or a young and educated 'techy' without previous convictions. Traditional criminal groups may also employ techy people to do the online aspect of the trade for them. Several researchers have mentioned such cybercriminal division of labour. Lusthaus and Varese (2017) found, for example, that online criminals can already know each other in person and may live in the same areas.

6.4 Discussion

Expert interviewees from law enforcement, government and the financial sector are a unique source of data. Their experiences in dealing with online fraud are generally not published, which makes their insights valuable. Several of such shared experienced show possible pitfalls in the behaviour of carders. In this section, interviewees' comments will be further explored in regards to the behaviour of carders, decision-making theory from Chapter 2 and previous findings of this work in Chapter 5.

Some of the overlapping behavioural pitfalls in the usage of tools by carders are listed below. These have been derived through interviewees' comments in this chapter and from the analysis in 5.3.2.

Behavioural	- Result-focussed

pitfalls	- Overconfidence and laziness - Trusting the wrong tool providers - Trusting the wrong people - Transcending online-offline boundaries - Inadequate obfuscation

Table 6.3 Classes of pitfalls

6.4.1 Result-focussed

Being too *result-focussed* has been identified as a behavioural pitfall in tool usage. Carders may adopt fewer security measures when they want to make a quick profit. VPN and PGP usage are, for example, tools that may not be used to improve efficiency (Sundaresan et al., 2016; Soska & Christin, 2015). Using these tools can be complex and time-consuming, especially for non-technical users, as stressed by various interviewees. They also stressed that cryptomarkets' will have policies promoting certain tools usage, but that these recommendations may not be followed-up.

Sundaresan et al. (2016) found that only 4.8% of merchant accounts on underground forums consistently use a VPN. The authors analysed Skype handles as, according to them, Skype is often used by cybercriminals to communicate with one another. They used a vulnerability in Skype, which allowed for the collection of user's IP addresses. They then used databases of a geolocation and online fraud prevention company[55] to map the IP addresses by country, Internet Service Provider (ISP) and ISP type. ISP types distinguish between cellular, residential, business, government and others. According to the authors, merchants that use mobile phones, instead of machines that consistently use VPNs, will care more about being available than about being secure. It is important to note that the study of Sundaresan et al. will most likely not be distributed in the same manner across all online criminals. The fact that carders

[55] MaxMind

in their analysed subset all shared their Skype handle is an indication that they value availability and usability over operational security, as they would otherwise not communicate via Skype but via more secure software, such as PGP. Therefore, the subset chosen is not representative for all kinds of online criminals. It thus is still important to consider users who use VPNs.

As we have seen in Chapter 4 and Chapter 5, the leadership of cryptomarkets often try to help their user base with staying secure by giving advice and integrating security mechanisms. They advice on, for example, tools, multisignature transactions, escrow, cryptocurrency tumblers, rating systems and automated carding shops (Eurojust & Europol, 2017; Horton-Eddison & Di Cristofaro, 2017; Europol, 2017). The leadership of cryptomarkets also often recommend to use PGP (Cox, 2016) and some have even integrated it into their markets' messaging systems. Time-pressure can affect System 2 thinking (Kahneman & Frederick, 2002). For result-focused actors, actions could thus become more automatic and associative, i.e. more System 1, when time is limited. This can affect usage of tools. Not using a SOCKS proxy or directly delivering a 'carded' product to one's home are also examples of being result-focused over secure. From a rational choice perspective, users would act according to the information available to them and thus comply with the leadership's advice. However, workarounds and non-compliance with policies, because of excessive cognitive load or distraction of main tasks, are factors that can stand in the way of 'optimal' decision-making.

6.4.2 Overconfidence and laziness

The behavioural pitfall *overconfidence and laziness* was also mentioned by various interviewees and is closely related to being *result-focused*. The result of the two pitfalls is the same: the usage of fewer secure tools. However, with *overconfidence and laziness* the carder is aware of the existence of secure tools, but simply fails to use them all. The necessity of using them will be underestimated, or temporarily dismissed. Using tools such as VPNs and not checking properly what user data they store can be an example of this. This is not a deliberate choice to obtain quicker results, or an unconscious effort by System 1, but a deliberate lazy choice of System 2. A user might already be aware that it is generally recommended to use certain tools and System 1 might intuitively remind him/her of this, after which system 2 decides on the quality of these intuitive judgements and whether to accept them (Kahneman & Frederick, 2002). However, for some users, the necessity of using the tools is not clear, i.e. not incorporated in their system 1 yet and automatically executed, which lets system 2 deal with it. Overconfidence and laziness may thus occur in those users who have not (yet) learnt that using certain tools is necessary. Furthermore, this can be influenced by systematic overconfidence in risk judgements (Sunstein, 1998). This implies that users will believe risks are more likely to materialise for others than for themselves.

6.4.3 Trusting the wrong tool providers

Proxy-enabled services sometimes cooperate with law enforcement agencies or are even run by them. Data sharing laws may also lead to the fact that such tool providers have to share data on customers when served with a warrant, even when they advertise not to share data with third parties. A failure to identify which tool providers cooperate with law enforcement is a possible behavioural pitfall for carders. If the development of a tool is stopped, such as TrueCrypt as discussed in Chapter 5, its usage might become unsafe. Furthermore, online criminals may be aware that they have to use certain tools to stay anonymous, but could be less aware that the default settings of these tools could still make them vulnerable. For example, in the Tor browser bundle, JavaScript is enabled by default. However, vulnerabilities in JavaScript have previously been used to deanonymise Tor users[56]. Status quo bias may lead to carders ignoring vulnerabilities and software updates, because they will feel comfortable in using the tools they have been using for a while. Also new developments, such as the adoption of multisignature transactions, may prove complex for members who are used to a certain set of methods, i.e. their personalised status quo.

[56] https://lists.torproject.org/pipermail/tor-announce/2013-August/000089.html

6.4.4 Trusting the wrong people

As was shown in the Chapter 5, carders often demand products to be delivered to drops. This is the same for many other online offenders, who, for example, deal in drugs. Addresses of these drops need to be sent to the vendor. Sending such information unencrypted or to the wrong person is a behavioural pitfall with possible consequences. Users may fail to identify that other users are scammers or undercover law enforcement, because of the anonymous environment they trade in (Décary-Hétu & Leppänen, 2013; Lusthaus, 2012). Law enforcement can surveil a drop once an address is accidently sent to an undercover agent. Also, (packet) mules who live at the drop, once arrested, may give up the address of a carder to law enforcement. Because of such risk, it was stressed that the rational fraudster would only use a specific drop for a limited amount of time. However, various interviewees stressed that cybercriminals sometimes use drops repetitively. This can be classified as status quo bias, but the endowment effect can also be influential here.

The endowment effect, which states that it is harder to give something up than the pleasure of having it (Thaler, 1980; Kahneman, 2011), may influence decisions on whether to keep a drop. It can also be an additional reason why vendors keep their username for a long time, even after marketplaces have been taken down, as they feel attached to its reputation. Loss aversion may also have relevance here, as getting rid of a drop can halt trade and thus lead to a possible loss of income. Risk-taking to avoid losses is central to prospect theory (Guthrie, 2002). Therefore, the carder may decide to keep a drop to avoid possible financial loss.

6.4.5 Transcending online-offline boundaries

Various interviewees mentioned the risk of ‘conversion points’ from the online to the offline world. They mentioned that cybercriminals will need skills in both environments. Whereas carders may have flawless online security, pitfalls may be encountered when they move into the offline or ‘real-world’ realm. As discussed previously, MAC addresses of devices can be used to infer locations or correlated with CCTV. Aldridge and Askew (2017) have similarly argued that for users of cryptomarkets key risks of detection is found in offline activities, such as packaging and delivering. Other examples in which online-offline boundaries need to be crossed include the converting of cryptocurrencies to fiat currencies and lack of legitimate sources of income, which can be seen as indicative signs for money laundering. These can cause specialised units to start (fiscal) investigations. A reference point of an offender will matter in dealing with such issues. As mentioned by interviewees, an offender with roots in organised crime, may struggle to stay anonymous online. However, he may have a network of offline mules to launder money. A technical individual who knows how to stay anonymous online, may, for example, forget that there is CCTV in place at ATMs. Their reference points will differ and so will, most likely, approaches to stay out of hands of law enforcement too.

6.4.6 Inadequate obfuscation

All of the behavioural pitfalls discussed above can lead to *inadequate obfuscation*. While users may follow the advice given on forums and consequently, for example, use a bitcoin mixer instead of directly cashing out, this could still lead to deanonymisation when they pick an ineffective mixer. Confidence in available information can thus sometimes be problematic for carders. Also, their lacking technical abilities, as mentioned by interviewees, might lead to the fact that they follow information available to them on forums incorrectly. For non-technical users, putting their trust in certain tools, or ‘expert systems’, without understanding them, is necessary to trade adequately (Ladegaard, 2017; Giddens, 1996). This can, especially if status quo bias is also in effect, lead to prolonged wrongful use of technologies, which might lead back to the real identity of users. Users may thus misinterpret available information.

6.4.7 Behavioural pitfalls and the analysis of online crime

It can be concluded from interviewees’ comments that various cognitive biases affect the behaviour of carders and other cybercriminals. The previously mentioned behavioural pitfalls have been examples of the various ways in which carders can make ‘irrational’ mistakes. Decisions are context-dependent. Culture, economic situation, local or offline status and many others factors determine whether individuals get involved in online fraud. A feeling of relative deprivation or boredom could lead to people getting involved from any origin or background. Ones off- or online surroundings will then influence the social learning process. This will determine how they will act in the illicit trade. While ‘optimal’ norms may be universally established on forums and marketplaces, local contexts may stand in the way of executing these. Access to Tor, cryptocurrencies or VPNs is, for example, banned in some countries, complicating adoption of ‘optimal’ norms for some carders. Therefore, much research can benefit from adopting cognitive biases, contextual factors and behavioural theories discussed in this chapter and Chapter 2 in their analyses of (cyber)crime. In this way, it will be able to better account for variations in offenders’ behaviour and commonly made ‘irrational’ mistakes.

Chapter 7 Expert interviews: the factors influencing policing and policy

Whereas the previous chapter has focused on interviewees' comments on the behaviour of carders, this chapter will look at a different element: the policing of carders. Particularly, this chapter's focus lies on the considerations of the interviewees in the addressing of carding, not on the carders themselves. The many factors that influence the policing of carding and other cybercrimes were of importance in this chapter and further explored. Formal and non-formal policies and considerations in such policing are also discussed throughout this chapter. Overall, its aim was to create a better understanding of the various factors that influence the policing of cybercrime, with a specific focus on carding.

The following remaining themes will be discussed below: *impact of carding*; *addressing of carding*; *cooperation, education and public awareness*; *trust in technology, legislation and culture*; *security vs. convenience*.

7.1 Thematic analysis of interview data

7.1.1 Impact of carding

The interviewees described the impact of payment card fraud in different ways. As the financial impact is very different across countries, the differences between interviewees in group 1 are not surprising. However, there were also noticeable differences between interviewees from the Netherlands, both from group 2 and 3. Several Dutch interviewees described the impact of carding as small [1, 5, 9, 16]. However, one Dutch interviewee saw its impact as large [3], while yet another indicated that there were, at the time of the interview, large investigations into carding with large impact ongoing [6]. Internationally, one of the interviewees mentioned that CNP has increased all over Europe and the U.S. Furthermore, the impact of carding was described as "high, very high" [19] and as something that "happens all the time" [17]. However, one interviewee from group 1 argued that it is decreasing [15].

Whereas the differences of opinion on the impact of carding are obvious between certain countries, the differences of opinion in one country are perhaps more surprising. This can be partly explained by the fact that interviewees from different sectors have different insights into the payment chain. Besides this, some parties benefit from presenting impact differently from what the actual impact is. One interviewee [12] stressed that banks prefer not to share fraud statistics and will only report it to card issuers (such as Visa or MasterCard) if they have the right to get a chargeback, i.e. when they profit from reporting it. Therefore, he argued, no fraud statistics are accurate, as many parties benefit from presenting lower numbers.

> "[…] the issuing banks, who are required to report fraud, don't always do so. Most issuers, as I know them, will think: 'how will reporting fraud benefit me? Did the transaction happen under such conditions that I can let someone else pay for it?' In other words, no one has fraud stats. They have them, but it is not correct. […] of course, they benefit from the fact that the world does not know that the actual damage is 1 billion, so they only report 500 million. Do you get it? That's what happens in the background."

Similarly, stolen cards will not show up in fraud statistics if they are cashed out at the cardholder's bank [1]. Additionally, [12] argued that there is still a lot of card fraud in the Netherlands with foreign cards, but that this also does not end up in fraud statistics in the Netherlands, as victims generally only report in their own country. Furthermore, issues around definitions affect fraud statistics [1, 4]. One interviewee [1] brought a confiscated iPhone to the interview to exemplify this. His company confiscated the smartphone, because someone had tried to buy it with stolen payment card details. The interviewee stressed that this can be classified as either cybercrime, laundering, scamming or handling stolen goods. Different parties in the payment chain can thus present fraud statistics in various manners, i.e. in whichever way it may benefit their goals.

Another issue for fraud statistics that was brought up by interviewees is that not all of it will be visible, as not all will be reported [10, 14]. In the Netherlands, if it is reported, victims will often be reimbursed. Paulissen and Van Wilsem (2015) found in an analysis of a large-scale survey of Dutch victims of identity fraud that, in the period of 2008-2012, more than 80% of victims were reimbursed. If they do suffer damages from identity fraud, more than 90% do not lose more than fifty euros. This shows that the impact on the consumer overall is generally not very large. Still, Paulissen and Van Wilsum stressed that banks and insurance agencies, unlike consumers, will suffer large financial damages. One interviewee [1] confirmed this for payment card fraud. Even when online criminals are not successful in their fraudulent attempts with Dutch cards and the financial impact of carding is not that high for consumers, it does not necessarily mean that the impact is low. Fighting payment card fraud still leads to a large indirect financial impact, as resources have to be invested to prevent it [1]. Therefore, the impact of payment card fraud is more than the fraud statistics that are available and will vary amongst stakeholders.

7.1.2 Addressing of carding

For this theme, the responses by interviewees are subdivided into two groups, as the motives for addressing payment card fraud and other online crimes will not always be aligned among law enforcement and government on the one hand and the financial sector on the other, as will become apparent.

7.1.2.1 Group 1 and group 2

Several law enforcement and government interviewees indicated that there is a fine balance between deterring criminals on the one hand and giving away too much information about their tactics on the other, which can be used by online criminals to learn how to stay more secure [9, 13, 14]. Law enforcement employs various traditional methods to fight online crime. Confiscating assets, i.e. monetary or illicit goods, is used for disturbing the criminal process [9]. It is also used to put vendors in a bad light by making sure they receive bad reviews as buyers will receive less products [13]. According to Europol (2014), the confiscation of criminal assets is integral to many investigations, but the usage of cryptocurrencies can severely complicate this process, as discussed in 6.3.

Furthermore, two interviewees from group 1 explained that law enforcement is quite often able to shut online criminal rings down, but that gathering enough evidence for arrests is difficult [16, 17]. This has, for example, been the case on hidden services on Tor, on which thousands of vendors are active, but when hidden services are taken down, generally only a relatively small number of users are arrested[57] [58].

When an online criminal marketplace or forum is shutdown by law enforcement, the original website is sometimes replaced by a message that it has been seized by one or several law enforcement agencies. These messages are often presented with the law enforcement agencies' logos, a mention of relevant laws and possible penalties when engaging in crimes related to the closed domain. Such interventions are, for example, part of the non-classified, i.e. publicly available, deterrence tactics of Europol (2014: p. 23). Europol argued that these "branded splash pages" can increase the impact of their successful operations to increase visibility, online presence and will lead to deterrence.

Two interviewees from group 2 said that Dutch law enforcement has adopted this tactic in a novel way to deter suspects on the darknet [8, 13]. The splash page created by Dutch law enforcement in late 2016 did not replace any forum or marketplace, but was a newly set-up .onion domain[59]. It listed vendors that have been arrested, but also pre-emptively listed active vendors, who were being investigated. It also mentioned the place of residence of some vendors, whose personal details were known to the police. This approach fits well with law enforcement's tactics of trying deanonymise users of darknet marketplaces, which was mentioned by one interviewee [13]. Some months after the interviews were conducted, in July 2017, Dutch law enforcement, in cooperation with international law enforcement, infiltrated and eventually seized a marketplace on

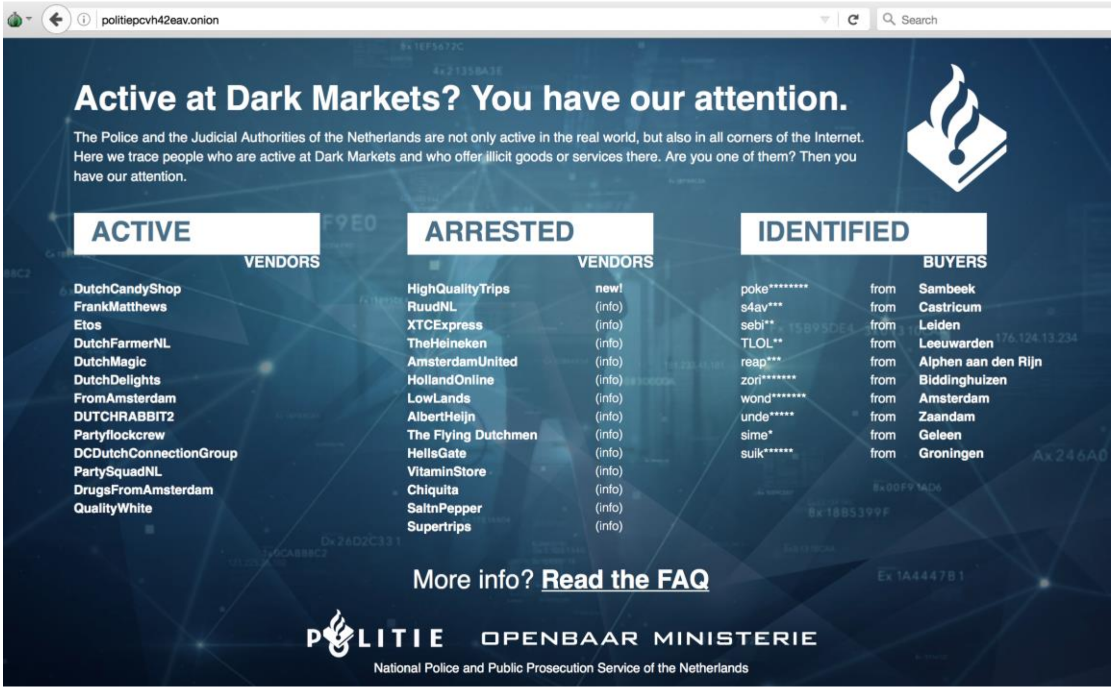
[57] For example, during Operation Onymous, an operation in which 16 European countries and the USA were involved, 17 vendors and administrators were arrested. See https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network.

[58] See https://www.gwern.net/DNM%20arrests for an estimate on the numbers of Tor darknet related arrests from 2011 to 2015. It must be noted that this number is incomplete, as the researcher only looked at arrest that have appeared in the English-language media.

[59] http://politiepcvh42eav.onion/

Tor. The .onion 'splash' page was subsequently updated to include a FAQ section on the seized hidden service[60]. On this page they explained to "have modified the source code which allowed us to capture cleartext passwords, PGP-encrypted order information, Bitcoins, IP-addresses and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace."

Dutch law enforcement, in cooperation with various international partners[61], infiltrated this marketplace after a FBI-led operation took down the largest darknet marketplace to date[62]. Displacement of users of the seized largest darknet marketplace was thus anticipated by Dutch law enforcement. Also, their updated 'splash' page shows law enforcement's focus on deterrence, as interviewee [13] stressed, by threatening to take user's anonymity away.



politiepcvh42eav.onion

Active at Dark Markets? You have our attention.

The Police and the Judicial Authorities of the Netherlands are not only active in the real world, but also in all corners of the Internet. Here we trace people who are active at Dark Markets and who offer illicit goods or services there. Are you one of them? Then you have our attention.

ACTIVE VENDORS	ARRESTED VENDORS		IDENTIFIED BUYERS		
DutchCandyShop	HighQualityTrips	new!	poke********	from	Sambeek
FrankMatthews	RuudNL	(info)	s4av***	from	Castricum
Etos	XTCExpress	(info)	sebi**	from	Leiden
DutchFarmerNL	TheHeineken	(info)	TLOL**	from	Leeuwarden
DutchMagic	AmsterdamUnited	(info)	reap***	from	Alphen aan den Rijn
DutchDelights	HollandOnline	(info)	zori*******	from	Biddinghuizen
FromAmsterdam	LowLands	(info)	wond*******	from	Amsterdam
DUTCHRABBIT2	AlbertHeijn	(info)	unde*****	from	Zaandam
Partyflockcrew	The Flying Dutchmen	(info)	sime*	from	Geleen
DCDutchConnectionGroup	HellsGate	(info)	suik******	from	Groningen
PartySquadNL	VitaminStore	(info)			
DrugsFromAmsterdam	Chiquita	(info)			
QualityWhite	SaltnPepper	(info)			
	Supertrips	(info)			

More info? Read the FAQ

National Police and Public Prosecution Service of the Netherlands

Figure 6.4 The .onion 'splash' page created by Dutch law enforcement

[60] http://politiepcvh42eav.onion/hansafaq.html
[61] https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
[62] https://www.fbi.gov/news/stories/alphabay-takedown

Various interviewees mentioned issues of responsibility, capacity and priority as factors that affect investigations. One interviewee argued that responsibility for security must be spread more over the whole payment chain, so businesses will pay more attention to fraudulent transactions and contribute more to fighting it [7]. Another interviewee from group 2 remarked that the Dutch police generally looks at whether there is a Dutch victim or perpetrator:

> "What we generally look at is: is there a Dutch perpetrator or victim? And if that is not the case, then it is often not relevant for us anymore." [8]

Capacity issues were mentioned as an issue hampering investigations by several interviewees from group 1 and 2 [8, 9, 14, 16, 17]. The changing nature of crime in the online realm was put forward as a reason for such issues:

> "It depends on the complexities of how the instrument works: it is international, it is very fast and it is partly anonymous. You need a lot more investigation powers to prove something." [14].

A lack of the right incentives, methods and manpower were also seen as a reason for why law enforcement is not able to "catch everyone", according to one interviewee [16]. It was further stressed that more vendors could be arrested if there was more capacity at a national level:

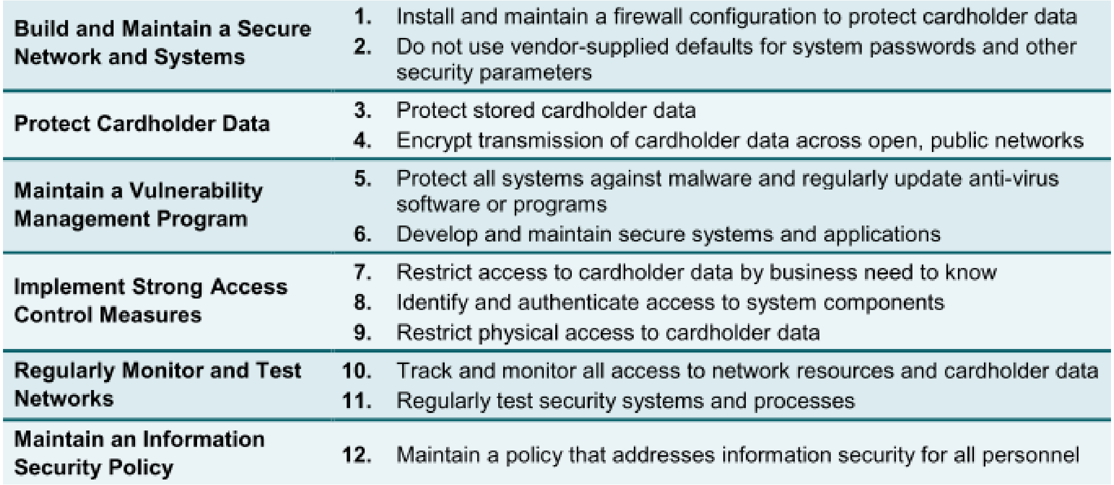
> "[...] the main bottleneck for many things we do here is not a mistake of the people [online criminals], but our own capacity [...] imagine if you are going to check for everyone: has this mistake been made? Hundreds of vendors will come out of that, but then what? Then we are sitting here with the two of us." [8]

One interviewee beliefs that investigations into carding do not have a lot of priority at the Dutch police [16]. Another argued that investigations into "big fish" on the darknet have priority, but if a murder case comes in, this will have priority and get most of the capacity [8]. Whereas there is always some information available, questions about how ‘deep’, how far abroad for example, one is willing to go in an investigation depends on the police leadership [14]. Priority at businesses will be very different from law enforcement, as issues of time may prevent them to invest in security [10], especially at small companies [17]. Also, businesses may look at risk and damage minimisation and not care as much about apprehending criminals, which one interviewee said to be unacceptable, as he prefers everyone dealing in accordance with the law [16].

Next to investigating card fraud after it occurred, the adoption of new technologies and the hardening of systems were frequently mentioned as ways of addressing (online) carding, mainly by interviewees from group 1. The uptake of EMV chip technology, which is the standard introduced by Europay, Mastercard and Visa that makes it harder to counterfeit cards than its predecessor, the magnetic stripe cards (Hayashi, Moore & Sullivan, 2015), was mentioned by interviewees as something that has helped in reducing payment card fraud [11, 15, 16].

> “Some years ago it was big and problematic, but then we moved from Stripe to EMV. That has solved the main part of the problems.” [16]

However, as payments cards have become more secure, the adoption of EMV has made the relative share of CNP in fraud statistics go up [11]. One interviewee also mentioned the strengthening of point-of-sale terminals and the ATMs infrastructure as successful measures which have led to the lower availability of stolen card details [15]. He argued that this number could be reduced further by a wider number of merchants being Payment Card Industry Data Security Standard (PCI-DSS) compliant. This is an industry standard that motivates all entities in the payment card processing chain who deal with cardholder and sensitive authentication data to “encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally” (PCI Security Standards Council, 2016: p. 5). In the PCI-DSS, the following twelve security standards are presented:



Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Figure 7.1 PCI Security Standards Council

The interviewee [15] stressed that if more entities comply with such standards and systems are “hardened”, carding is prevented. Tackling the card vendors is the wrong approach, he argued, as card details can be replicated and spread by anyone. Making sure they are not available in the first place is more important. Another interviewee from group 1 argued that in the future online trade needs to happen through more verified means as this will also reduce the opportunity for vendors to steal card data [17].

7.1.2.2 Group 3

Whereas the interviewees from the Dutch financial sector talked in a similar fashion about some aspects of addressing the issue of carding, their focus lied more on the adoption of secure technologies and in making sure less card details are available. Similar to interviewee [17], interviewee [1] stressed that, in the future, improved authentication of users will be important in online transactions. Also, he mentioned that the disappearance of the static password, in accordance with the second directive on payments services (European Parliament & European Council, 2015), will further complicate fraudsters’ illicit activity. Instead, one-time passwords will have to be generated, which should increase payment security. In line with this, one interviewee argued in favour of a wider adoption of two-factor authentication by smaller online merchants [3]. A two-factor authentication code can still be stolen, but this would make the type of fraud, which was classified as

CNP before, phishing, according to two interviewees [3, 4]. They also stressed that online fraud detection in the Netherlands is already working so well that fraudsters have recently shifted their focus towards trying to obtain physical cards and pin codes again.

One interviewee stressed that the adoption of security measures does generally not run parallel across countries, which is abused by online criminals, as they can move between them [12]. European institutions seem to be aware of this, which can be derived from the fact that new measures have to be adopted by member states within a certain timeframe. The second directive on payments services had, for example, to be adopted by European member states by the end of 2017. The interviewee exemplified how non-parallel adoption can otherwise lead to issues for late adopters.

> "… if a jeweller on the PC Hooftstraat [famous shopping street in Amsterdam] makes 100.000 euros a month and an American counterfeit card ends up being used there, maybe from the dark Web, well, our terminal is EMV, we can handle a chip, that those Americans still have an old magnetic strip: that's their problem. And by the way, a transaction means money for us." [12]

In relation to traditional policing methods, an interviewee mentioned that arrests can be a very successful method to reduce fraud. His company noticed one specific fraud type going down by 80% after just one arrest [1]. Finally, similarly to observations made in group 2, one interviewee noted that at court cases involving cybercrime, when banks or law enforcement have to explain how they ended up with a suspect, there were dozens of known criminals in the public stands who were all there to learn. Law enforcement agencies therefore have to think about to what extent they can publicly hide their detection methods, as online fraudsters will otherwise simply learn about them and evade them [3].

7.1.3 Cooperation

Another issue in addressing carding, is the fact that online crime is often committed across borders. Different sectors, i.e. public and private, will often have different kinds of information on suspects. Several interviewees therefore mentioned the necessity, but also the struggles, of international, intercultural and intersectoral cooperation.

Several interviewees argued that there is almost always some kind of international component in cybercrime cases. Therefore, international cooperation is essential. This is increasingly going well, some argued [8, 13].

> "There's no more borders. Not tangible anyway, so you have to cooperate with each other. Exchange information, look for the connection. That happens in this area. You can try to keep everything to yourself or be difficult about it, but uhm, every vendor sells to various countries, there is not one that focuses on one country." [13]

Because of increased international cooperation, processes that used to occur several times across law enforcement agencies, now only have to happen once [14]. Mutual legal assistance was seen as an issue among interviewees, as it is necessary, but can significantly slow down investigations [4, 6, 8]. The Budapest Convention on Cybercrime (2001) was mentioned as a facilitator of quick cooperation that can be used before any mutual legal assistance requests are sent to formalise the process [7]. This is needed, as responses to formal legal assistance can, according to one interviewee, take up to six months [8]. Other interviewees confirmed this, as requests for mutual legal assistance may end up in a "black hole" in some countries [5, 14]. Many tool providers, such as VPNs or bulletproof hosting, are aware of this and purposefully base themselves in "annoying", i.e. non-cooperative, countries [7]. Such legislative barriers in international cooperation need to be overcome with mutual legal assistance treaties (MLATs), argued yet another interviewee [19]. Also, he further argued that

National Central Bureaus (NCBs)[63] of INTERPOL can help facilitate such matters. Complete global cooperation was mentioned by several interviewees as a “utopia” and a “good big brother” in the fight against online payment card fraud [5, 11]. However, issues with such approaches were also mentioned:

> “[…] of course, a global database, a global, a good big brother, would be very helpful. We could in zero time have all the cross-matched information and many of these risks would be avoided. But this is, I would say, related to science fiction, as it’s already quite difficult to agree between EU member states on some matters. Just imagine how it would be possible in reasonable time to make all the world agree.” [11]

One interviewee also argued that there will always be a place for fraudsters to work [5]. Still, another mentioned trusted global intelligence sharing platforms across law enforcement agencies as a future solution to such issues [18]. Cultural and geopolitical issues can, however, stand in the way of sharing information on an international scale. Some nation states value their sovereignty over potential cooperation [8, 11]. Non-cooperative banks, located far away from Europe, were also mentioned as an issue by an interviewee from group 3 [4]. Fraudsters are sometimes aware of these situations and may move away to countries with worse security measures than where they were originally based [12]. One interviewee stressed that there are not just procedural, but also cultural barriers in cooperation. For example, people in some countries may sometimes not work on the same days for various reasons, which can lead to a delay in receiving information [18].

Several interviewees from group 3 argued that the collaboration between banks and law enforcement in the Netherlands is working well and necessary in getting convictions [1, 2]. As one interviewee stressed:

[63] https://www.interpol.int/About-INTERPOL/Structure-and-governance/National-Central-Bureaus

> “If you look at court cases in the last one or two years […] people who have in recent years really been convicted for cybercrime, this is purely because of the success of cooperation between law enforcement and banks.” [1]

Sometimes such cooperation only leads to the arrests of money mules, [2] stressed, but this is a starting point from which it is possible to continue investigations. One interviewee called this cooperation necessary, as payment card fraud is a societal issue that needs to be solved with both public and private institutions [3]. Two interviewees stated that Dutch major banks do not compete on security and share threats among each other [4, 16]. This is exemplified by the Dutch Electronic Crimes Taskforce (ECTF), a collaboration between law enforcement and major banks in the Netherlands. Such collaborations also exist in other countries and even on a global scale, such as through the Financial Services – Information Sharing and Analysis Center (FS-ISAC). A combination of the current measures in place at Dutch banks and the success of their cooperation through ECTF is the reason why fraud with Dutch cards at Dutch institutions almost disappeared, argued one interviewee [14]. Other entities, such as payment processors, also cooperate with various parties to contribute to fighting payment card fraud, as they have a good oversight of payments [12]. Cooperation between law enforcement with such entities in the financial sector needs to get better in the future, according to [18].

7.1.4 Education and public awareness

Several interviews argued that education is both required for professionals fighting online crime and for potential victims. One interviewee stressed the necessity of the training of technical law enforcement agents to fully understand complex online environments and cooperation with social scientists to understand all the types of exchanges, on for example the darknet [10]. Education for prosecution services and judges on cybercrime was also deemed necessary, argued one interviewee [18] in line with the Council of Europe (2017). According to [11] and [18], the education of the public about the usage of security measures is crucial in reducing the overall loss of money. International law enforcement agencies, such as Europol, have as its task to educate and raise awareness among the European citizen when it comes to these issues, [11] said. Next to the education of the public, the spreading of awareness about responsibility amongst merchants, government and card issuers is also important [3, 7]. This could spread the costs for fighting fraud across sectors.

> "[…] spread the responsibility of taking care of security over the whole chain. Then people will start to pay attention. Then companies will start to pay attention and do more." [7]

7.1.5 Trust in technology, legislation and culture

Understanding a country's payment culture and legal situation is important for understanding the types and amount of fraud in that country [4, 8, 11, 16]. A decline in trust in technology can be a consequence of fraud, several interviewees argued [6, 7, 11]. This risk is not easy to measure, but still important to consider. Online criminals, similarly, might lose trust in anonymisation technologies after they see other users being arrested. Changes in legislation can be necessary to make businesses comply with safer methods. This consequently can lead to less fraud, more trust in technology and a safer payment culture, which is why these three themes are grouped together.

When it comes to the consequences of fraud, the key issue is trust according to one interviewee [7]. Individuals who have been defrauded lose trust in payment systems [6]. [11] stressed that issuers and banks might forget about such consequences, as they do not show up in their fraud stats.

> "Maybe the losses are not significant to them [issuers and banks], but it is, it will be significant to acquire new customers or to convince these people that the method of payment is still trustworthy." [11]

Credit cards were described as an ancient method from a cybersecurity perspective by one interviewee [16], as a fraudster only needs the numbers on the card. [14], similarly, argued that cards will disappear as a payment method and that biometric and phone payments will take over. [11], however, feared the unchangeability of biometric information, which could lead to identity theft. Interviewees from group 3 did not make any comments about a potential loss of trust in technology.

The payment culture of a country is important to understand its types and levels of fraud. For example, in the Netherlands people do not use credit cards a lot because of the prevalence of IDEAL [8, 16]. Therefore, the Netherlands is relatively secure in the global market [10]. One interviewee stressed the uniqueness of the Netherlands:

> "[…] the Netherlands is actually a very weirdly exceptional country when it comes to credit cards. That is because our culture I think, because we find it very unnatural to spend money that you do not own. Seems healthy to me, Calvinistic. But as a consequence, at most shops, you can't use that thing [credit card]. Also not at the supermarket, to the great frustration of most tourists in the Netherlands." [16]

Because of the differences across countries, traditions, cultures and legislation, addressing fraud is a complex matter [18]. Also, differences in policing culture matter in determining if and how swiftly cases are dealt with, according to one interviewee [4]. The socio-economic situation of certain nations with, for example, high unemployment rates, was also mentioned as a cause of fraud. [19] said that, in his country in West-Africa, students are even approached when they graduate university to get involved in online fraud. [18] further argued that many people were interested in carding in his nation in Eastern Europe, because of the following reasons:

> "Easy profits, probably also the economic situation in the past was not that good in our country, uhm, so it was an easy profit, for some people it was just a way of living, it was cool to have money instantly. And to be socially admired let's say. … these kinds of crimes [carding] are not,

> generally speaking, heavily punished … It's difficult, I would say social factors, economic factors, social, they are innovative with social engineering, clever, morality a little bit. Many factors." [18]

According to one interviewee [5], these are exactly the things that need to be fought. The societal perceptions of openly rejecting "when people enjoy unlawfully obtained money" in more societies would be helpful in solving the issue of (online) fraud.

Several interviewees mentioned positive and negative issues in current legislation which affect addressing carding. One interviewee [16] pointed towards the fact that the reselling of someone else's information, such as payment card data for example, was not illegal in the Netherlands until July 2017 when the law 'Computercriminaliteit III'[64] was adopted. Interviewee [3] argued that legislation that forces online shops to use two-factor authentication should be enforced, maybe even on a European or global scale. If such legislation is not adopted on an international scale, fraudsters can simply displace their activities to another country. Differences in legislation internationally were also mentioned as an issue [5]. In the Netherlands, authorities can act on fraud signals on fiscal grounds, such as "inexplicable capital", when there are indications that someone is engaging in money laundering. This may be different in other countries and can be complex when asking for assistance, [5] argued. In other areas, policy is created at a European level to make countries comply to the same standards and to facilitate international cooperation. For example, the European Parliament wrote in one of their directives that "competent authorities should be able to monitor the use of virtual currencies" (2017: p. 8) and that "virtual currencies cannot be anonymous" (2017: p. 102). In this way, it appears that the European Parliament supports deanonymisation efforts by member states.

[64] https://www.eerstekamer.nl/wetsvoorstel/34388_wet_gegevensverwerking_en

7.1.6 Security vs. convenience

Various interviewees commented on how convenience in online shopping is important for businesses and their customers. However, this may affect the security level of transactions and consequently lead to more fraud going unnoticed. Several interviewees from group 3 argued to various degrees that customers should not be overly bothered with security measures, even if it can reduce fraud, as customers see the measures as inconvenient [1, 3, 4, 12]. Two interviewees from group 1 and 2 similarly stressed that there has to be a balance between security and convenience [5, 11]. One interviewee described the approach of his bank as follows:

> "I still believe that every euro of fraud is one too many, we are very fanatical in that, but if I make the fraud very low, but because of that make it incredibly difficult for my customers, I might have a larger loss, because I lose customers, then, yeah, in the end we are a commercial company" [4]

Card fraud cannot be completely eradicated, except if extreme measures are taken, such as getting rid of credit cards as a payment method, [4] argued. Furthermore, he stressed that in fighting fraud 99% of people suffer for the 1% of transactions involving fraud, comparing it to an extreme Pareto, which states that 20% of the cases determine 80% of the outcomes (Juran, 1954). Another related issue is the non-parallel adoption of secure technologies across online merchants.

Companies can decide not to implement certain technologies, such as 3D secure, as this may lead to more customers who find competitors who do implement security measures inconvenient (Hayashi, Moore & Sullivan, 2015). Several interviewees [3, 4, 12] mentioned non-parallel adoption and consequent loss of customers to be an issue. Fraudsters profit from these kind of market games, [12] stressed. [12] furthermore explained that some online merchants may deliberately accept fraudulent transactions, as convenience of use can lead to higher profits. [3] stressed that the adoption of two-factor authentication should therefore be mandatory, as fraudsters can otherwise spend the entire balance of a card. Online merchants "hide behind automation" as they sometimes send lots of packages to the same address without question, which could easily be detected as fraudulent, according to [12]. Another issue mentioned by an interviewee [2] is same-day delivery of products, as the response to intercept such packages, if the transactions were fraudulent, has to be very swift.

7.2 Analysis of interviews

The experiences of expert interviewees shared in this chapter showed possible chances and pitfalls in the policing of cybercriminals, particularly carders. In this section, previously discussed comments will be further explored in regards to the behaviour of carders, criminological literature and previous findings in this work.

Different stakes at play determine how various parties represent fraud statistics. Several interviewees questioned published statistics. It appears impossible to calculate a completely objective *impact of carding*. Definition issues can, purposefully or not, lead to different representations of losses caused by fraudulent activity. Also, underreporting by both institutions and consumers lead to wrongful statistics. Whereas companies' reputations may benefit from presenting lower fraud numbers, underreporting could be detrimental the addressing of fraud. An increase in reporting would inform law enforcement better and can help in deciding how to effectively allocate resources (Bidgoli & Grossklags, 2017). Interviewees also mentioned costs made to prevent fraud as an element which will generally not be part of fraud statistics, but will still be a significant investment for companies.

Several interviewees mentioned that arrests and prosecutions can have the negative consequence of providing (future) online criminals with the chance to further educate themselves on how to stay secure. This has also been shown in other research. For example, the uptake of more secure methods, such as PGP, increases after large law enforcement takedowns of hidden services on Tor (Soska & Christin, 2015). According to Ladegaard (2017, p. 15), media reports presenting law enforcement's activity in fighting cryptomarkets trade failed to "lift actor's subjective perception of risk, and ultimately did not deter trade". Furthermore, takedowns of cryptomarkets were not considered an effective measure to reduce sales on illicit (drug) markets, according to Décary-Hétu and Giommoni (2017). Because the cryptomarkets ecosystem seems resilient in the long term against takedowns by law enforcement, Soska and Christin (2015) argued for the adoption of novel measures focusing on prevention. Previously discussed operations by Dutch law enforcement involved cryptomarket infiltration at a high level and anticipated displacement before taking down the marketplace. This shows that law enforcement agencies are aware of the limitation of taking down one marketplace at a time. Also, the use of ‘splash’ pages in which vendors on the darknet are ‘named and shamed’, is a novel measure. Such approaches might prove to be more fruitful in the long term than standalone takedowns. Future research will have to examine this.

In connection to this, international and intersectoral *cooperation* has generally been deemed essential for effectively addressing cybercrimes on the darknet (Europol, 2017; Omand, 2015; Buxton & Bingham, 2015). Several interviewees in this work also mentioned the necessity of cooperation. Some, however, focused on its difficulties, as it can be very complex, because of issues such as sovereignty, time, mutual legal assistance, differences in culture and priority. Eurojust and Europol (2017: p. 11) have raised similar concerns. They stated that the “current differences in legal frameworks and ineffective international cooperation may lead to the emergence of online criminal hot spots and (virtual) safe havens, where investigations and prosecution as well as evidence collection are challenging". They aim to solve these issues in the future on a EU-level by creating cooperation frameworks for the collection and exchange of information in cybercrime investigation, prosecution, prevention and protection. The Budapest convention is already trying to do this and can be a useful legislative tool to facilitate cooperation between states. Still, various issues persist in mutual legal assistance in accordance with the Budapest Convention. Workload, complex procedures, time, delays, language issues, sheer quantity of requests and different legal thresholds were mentioned as standing in the way of success, amongst several other problems (Cybercrime Convention Committee, 2014). In future research, cognitive biases influencing international cooperation could be examined to better understand this issue. Also, not every country can or wants to join the Budapest Convention, respectively because of capacity issues or political objections (Clough, 2014).

Across sectors, there are even more possible issues. Law enforcement agencies may have different concerns in addressing cybercrime than, for example, banks. This difference became apparent in various interviews. Interviewees from the financial sector look at the customer's point of view and their own financial incentives. They do not want security measures to stand in the way of their customer's convenience or the usability of their services. This leads to the acceptance of some fraud to occur. An example of this is the adoption of 3D secure. Financial institutions could reduce fraud by doing this, but when a competitor does not adopt it, it could lead to a loss of customers (Hayashi, Moore & Sullivan, 2015). However, another concerns for the financial industry is the decrease of trust in their technologies because of increased fraudulent activity. Law enforcement agencies, on the other hand, operate from the perspective that everyone who commits fraud should be arrested, in principle. However, realities of capacity stand in the way of such objectives. Therefore, the fighting of fraud will generally be focused on the 'big fish'.

The fighting of cybercrime operates at several levels. *Education and public awareness* are a part of this. Governmental agencies and (inter)national law enforcement educate the public on cybersecurity issues through campaigns. Sometimes these are organised from an international group of public and private partners, such as the 'No More Ransom' campaign[65]. However, such initiatives are often organised on the national level, such as 'Take Five'[66] in the UK. More targeted campaigns to prevent young people getting involved in online crime have involved collaborations with the video gaming industry and sending cease and desist letters to "those on the periphery of cyber crime" (NCA, 2017: p. 3).

Several interviewees stressed the importance of culture and localities in understanding (online) fraud. Analysing local settings with the square of crime can explain why carders from a certain country are active in another. For example, if one nation has a weak economy with not enough fitting jobs, people might become fraudsters and target victims from more economically thriving countries. Lusthaus and Varese (2017) exemplified this in their case study of Romania, which can only be understood by seeing it in its national context. The

[65] https://www.nomoreransom.org/en/about-the-project.html
[66] https://takefive-stopfraud.org.uk/

legacy of secluded communist politics, economic development and corruption/protection were mentioned as part of this context, which enabled fraud to thrive. Also, as there are many job opportunities for technical roles, the focus of online crime in Romania is more on online fraud, which is generally not as technical as, for example, malware or hacking. Countries of which victims are commonly targeted, such as the United Kingdom and the United States, have consequently expanded international cooperation efforts with Romania (Europol 2015, 2017; Lusthaus & Varese, 2017). A square of crime approach can in this case contribute to reducing displacement, as it can help in analysing the consequences the context of crime in a multidimensional perspective. This shows that contexts have to be considered when addressing online crime.

Varying legislations across countries can affect the size and success of online criminal activity in a certain region. Legislation streamlining efforts are therefore being undertaken at international levels (Eurojust & Europol, 2017). Furthermore, training, technical assistance and capacity-building efforts are employed against international online crime by international overarching organisations (INTERPOL, 2016; UNODC, 2016; Europol, 2017). Such legislative and capacity-building efforts try to unify countries' approaches in fighting online crime, which, if successful, can lead to a reduction in fraud, more secure payment cultures and increased trust in technology. However, as previously mentioned, there are many complexities in such initiatives which can hamper successes.

7.3 Discussion

In this chapter it was shown through interviews with experts that the addressing of online crime, specifically carding, is a complex process affected by a wide range of stakes at play. Capacity, priority, usability of services, cultural differences, and human and financial resources are some examples. These stakes varied across groups of interviewees, mainly between group 1 and 2 on the on hand and group 3 on the other. However, there were also some minor differences between interviewees from group 1 and 2. Group 1 was generally more positive on the effectiveness of international cooperation, while interviewees from group 2 commented more on the inertia of processes of international assistance. Law enforcement and government interviewees commented on the fact that they look for flaws in suspect’s behaviour and in the technologies they use. They thus look for mistakes in the modus operandi of online criminals. Furthermore, they cooperate with various parties to increase chances of finding such flaws and accelerating this process. Law enforcement uses innovative tactics to try and reduce the issue, but sometimes such measures are counter effective and simply lead to displacement and increase criminal innovation. The adoption of new technologies by criminals, increased operational security measures, problems in cooperation (speed, cultural) and priority (budget, capacity) are all issues that can stand in the way of successes in fighting cybercrime.

The interviewees’ comments show that all parts of the square of crime, as discussed in 2.3, are important in the criminalisation process and in thinking of possible countermeasures. Offline communities, national payment cultures and efforts by law enforcement agencies and other financial and security companies will determine how likely individuals are to get involved in online fraud and how successful they will be, according to several interviewees. Also, online communities will influence the decisions of fraudsters. Their decisions can be informed by tutorials, which may or may not be up-to-date with perceived optimal paths. However, they might also work according to tactics which have previously proven to be effective, but may no longer be, i.e. status quo bias might be in effect. An example of this is trusting platforms or technologies which were secure, but can, for example, be covertly taken over by law enforcement.

The decision-making of both law enforcement and government officials on the one hand and financial industry experts on the other will be dependent on the information and resources available to them, but also on their motivations. As interviews in this chapter have shown, the financial industry’s focus is broader than the reduction of fraudulent activity, as the usability of their services needs to be upheld in order not to lose customers. Also, their (lack of) motivations in reporting fraud can affect other parties’ efforts of addressing fraud. Similarly, law enforcement agencies or other government parties may or may not address fraud sufficiently depending on a political context, which, for example, demands a larger focus on other crime areas. Therefore, the context in which decisions are made is crucial to understand. Future research needs to further explore this. Available information will affect decision-making, but as was shown in this chapter through interviewees' comments, a wide array of other influences determine how decisions are finally made.

Chapter 8 Conclusions and future work

Throughout this thesis, the illicit online trade in stolen payment card details has been explored from various angles. Insights into the behaviour of carders have been obtained both through analyses of data produced by carders themselves, i.e. tutorials, and by interviewing law enforcement, banking and security industry experts. A review of the literature was also used to analyse the tools that carders were found to employ. The combination of methods used in this thesis has led to realistic insights into the behaviour of carders. First, a recap of the contributions per chapter is presented below. In doing so, it will be shown how this research has attempted to answer its research questions (see 1.5). From this, the overall contribution of the thesis will be discussed. Finally, some possible limitations and avenues for future work arising from this thesis will be discussed.

8.1 Summary of findings

First, to show the most commonly taken steps in carding, a crime script analysis of the illicit use of stolen payment card details was created. This script was created from 25 carding tutorials that were found on a, now defunct, cryptomarket. It has shown which tools were most commonly recommended in the carding process. This led to the creation of a six-scene carding crime script. Furthermore, insights into several methods in which funds from stolen card details are laundered were derived from the 25 tutorials. The crime script allowed for the creation of possible situational crime prevention measures. In a discussion on the potential effectiveness of these measures, it was stressed that these measures will have to be adopted on a mass scale, perhaps even globally. This is the case, as they might otherwise simply lead to displacement. Some of the proposed situational crime prevention measures may have the side effect of affecting business and citizens. This is the case, as many of the tools used by carders also have legitimate purposes. A better understanding of the tools identified in the crime script was therefore deemed necessary. Specifically, the processes carders go through needed to be better understood to find possible weaknesses that can contribute to prevention and interception.

The organisation and tasks involved in carding were therefore further explored with the CommonKADS method. The different steps of the carding process were analysed to see how important they were in the process, how they were connected and what tools were used in which steps. The possible bottlenecks of utilising these tools were then laid out for the categories *proxy-based services*, *cryptocurrencies* and *physical*. It was also discussed at how the utilised tools may affect. This has enhanced the crime script analysis by adding more detailed insights into the organisation and tool usage of carders. Furthermore, Chapter 5 added context to why carders, and other cybercriminals, would use such tools. Whereas in the crime script analysis an optimally recommended path of crime commission is presented, the exploration of the organisation and tasks involved in carding with the CommonKADS method has revealed possible weaknesses in tools. Those latter findings have shown that carders can encounter many bottlenecks and generally cannot be certain of staying fully anonymous. Therefore, this thesis has argued, cybercrime research needs to include such possible pitfalls in its analyses, in order to present decision-making more accurately.

Expert interviews were used to get insights into the decision-making of carders that could not be obtained from public data. Several expert interviewees verified that carders often act irrationally and can be arrested because of non-optimal use of available technologies. Their comments have shown that carders are often influenced by cognitive biases. The interviewees stressed the importance of some of the findings of this work, i.e. that online criminals are often not rational in their decision-making and that such flaws in their behaviour and bottlenecks in tools may be used to deanonymise them. Interviewees, however, also stressed that a wide range of stakes at play will influence whether carders, or other online criminals, can be apprehended. Many factors complicate their investigations and can stand in the way of the prosecution of cybercriminals. Examples of these include financial resources, priority in investigations and international cooperation issues. Therefore, even if a cybercriminal can technically be deanonymised and arrested, it will not always occur.

While mistakes and technical bottlenecks thus do not automatically lead to the apprehension of carders, they are important to map as they can contribute to thinking about interceptive measures. However, as various interviewees stressed, arresting the carder is not the only element that needs to be focused on. Therefore, it has been argued in this thesis, that an approach that addresses the four pillars of the square of crime should be used. While mistakes by offenders need to be exploited, opportunities for victimisation and displacement also need to be minimised. Efforts to strengthen the storage of payment card data and to consequently protect consumers and minimise fraud are already ongoing in international environments. An example of this is the PCI-DSS (PCI Security Standards Council, 2016). If more merchants globally become compliant to such standards, merchants will stop storing certain types of sensitive data, such as, CVV or PIN codes. Consequently, compromised payment card details will become less useful for fraudsters. Smaller merchants are less likely to be PCI-DSS compliant than larger ones (Hayashi, Moore & Sullivan, 2015). This shows that there is room for improvement there, just as in the international adoption of security mechanisms. Currently, international displacement enabled by the borderless environment that is the Web is too straightforward. Security mechanisms, such as 3D secure, can easily be avoided by spending stolen card details at ecommerce platforms where such measures are not mandatory yet.

Because of the international nature of carding, and much other cybercrime, a holistic approach is needed in addressing it. This is both important for prevention and interception. A law enforcement agency can takedown a forum or marketplace on which stolen payment card details are traded, but this is a temporary situational crime prevention solution to a larger issue. Effective solutions will have to be taken in tandem with various parties with wide reaching interests. In accordance with the square of crime, general measures for the individual pillars can be created to reduce carding overall. First, guidelines need to be established to enforce security mechanisms, such as two-factor authentication, on ecommerce websites. This can in many cases prevent carders from cashing out stolen payment card details and will consequently protect the cardholder, as they will then also need to obtain the second factor next to the card details. Second, international cooperation treaties need to be established between all law enforcement agencies internationally. In this manner, international investigations can be streamlined, making it harder for the fraudster to displace. Third, international guidelines need to be established on the reporting of data breaches. Whereas countries may have national legislation on such issues, leaked data can be used internationally. This makes it essential to allow the public, i.e. cardholders, aware once their data is leaked to take measures to prevent their data from being abused.

There are many obstacles in working towards such effective international solutions against carding. As we have seen from interviewees' comments in Chapter 7, these include, amongst others, nations that value sovereignty over cooperation, definition issues of cybercrime and the adoption of security measures and new card schemes. Furthermore, larger national and international economic issues are also relevant, as these can contribute to a rise in fraud. More specifically, as this thesis has shown, the (novel) methods and decision-making by carders also need to be better understood, as these determine to what extent international cooperation, guidelines and streamlining is necessary in the addressing of carding. Overall, the pillars of the square of crime and the way they have an effect on each other need to be kept in mind. In this way, a holistic understanding can be created that minimises displacement, as it will consider the various elements for which countermeasures against carding need to be designed.

8.2 Contribution

This research has contributed to a better understanding of the decision-making of cybercriminals. This contribution has both been empirical and theoretical. The analysis of carding tutorial data and expert interviews' comments has been the empirical contribution of this work. By creating a crime script analysis from 25 tutorials, novel insights were obtained on commonly advised paths of online crime commission for carding. By critically judging the effectiveness of situational crime prevention measures, derived from the crime script, further analysis with CommonKADS was justified. This method proved a useful extension on the original crime script, as its models allowed for an in-depth analysis of possible bottlenecks in tools used by carders. This has shown some of the possible ways in which carders can make mistakes in the carding process. Comments by expert interviewees have further shown that carders are influenced by various cognitive biases and contextual factors. These can affect their decision-making and, consequently, lead to their deanonymisation and possible apprehension.

The theoretical contribution of this work has been shown through the combination of methods that have provided a novel approach in the analysis of cybercrime. Models of expected utility and rational choice, on which crime script analysis and situational crime prevention are based, often provide interesting and valuable insights into the most common ways in which (cyber)criminals commit crimes. Such methods have proven to be popular (as shown in 1.3). However, they may overlook deviations from such norms. Decision-making is often influenced by contextual factors and cognitive biases. These stand in the way of the maximisation of utility. This thesis has identified and identified several of such cognitive biases through the usage of CommonKADS models and expert interviews. These have shown the different manners in which carders, and online criminals more generally, can fail to act rationally in accordance with available information. Consequently, cognitive biases can lead to mistakes that, in turn, can lead to the deanonymisation of carders. Furthermore, even when carders use tools in a perceived optimal manner, technical bottlenecks in tools they use may lead to their deanonymisation and possible apprehension. The analyses in this work have shown that mapping such biases and contextual factors can contribute to the understanding of cybercriminal behaviour.

Furthermore, this thesis has obtained novel into responses by law enforcement agencies and other parties to minimise the threat posed by carders. From the analysis of expert interviewees' comments, it has become apparent that the square of crime is a useful tool for the analysis of carding. It can be particularly helpful in demonstrating why carders operate in a certain way and in thinking about countermeasures. This is the case as rationalisations for cashing out stolen payment card data will differ based on context and locality. For example, there will be more possible victims in certain countries, because of old card schemes being in use or a relatively wealthy population. Other countries may have more skilled attackers, not enough fitting jobs, more acceptance of corruption and less law enforcement presence (see, for example, Lusthaus & Varese, 2017). Still, as security behaviour also differs across cultures (Sawaya et al., 2017), the assumption of what rational individual security behaviour is also does. In other countries, law enforcement may be insufficiently capable to deal with online crime or have no cooperation agreements with certain countries in addressing international (online) crime.

Societal contexts can thus have a significant influence on policing processes, security behaviour, victimisation and populations' chances to show its discontent with levels of crime. Therefore, the square of crime needs to be kept in mind for meaningful modelling efforts of crime to explain the interactions between its four pillars and, consequently, the social context in which a crime is committed. 'Bounded' rational choice models, used by situational crime prevention and crime script analysis, are therefore only useful in part. This is the case, as they argue that decision-makers act according to the information, time, and skill available to them. While this is true, this overlooks other cognitive biases and contextual factors identified in this research (see 6.4) that may be of relevance in the analysis of cybercrime. To analyse the decision-making of cybercriminals more accurately, these need to be taken into account. Such an improved understanding can lead to better countermeasures. This better understanding of the offender can, in turn, influence all the other elements of the square of crime positively too, by leading to less card fraud, which decreases the number of victims and can make the public regain trust in law enforcement agencies and card issuers.

8.3 Limitations and future work

As previously discussed in section 3.8, there are various possible limitations to the data used in this thesis. While novel, the usage of tutorials as a source of data evoke similar questions that much other types of data for qualitative analysis encounter. An example of this is whether the amount of tutorials analysed is the right amount. This concern can, similarly, be raised for the number of interviewees participating in this work. However, this research sought to understand the behaviour of decision-making by carders in-depth, rather than in-breadth. Generalisability can thus be seen as a limitation of this thesis. Still, the number of tutorials used is justifiable for this thesis, as generalisability was not its purpose. Future work could attempt to collate larger amounts of tutorials, in various languages, for analyses. This could, for example, lead to research that looks at the evolution in carding tutorials over the years, linguistic analyses to find the most commonly recommended tools and techniques across different languages, and quantitative analyses of how many tutorials have been bought across marketplaces and forums.

While recruiting expert interviewees in this field is complex because of accessibility issues, the amount of expert interviews in this thesis is justified as data saturation for the purpose of this research was reached. The amount of interviewees, combined with their unique insights, contributed to the novelty of this research. Future research could take a quantitative approach and, for example, distribute surveys across law enforcement agencies. Such an approach could be used to ask a wide variety of participants what the complicating factors are when investigating cybercrimes, on local, regional, national and international levels. Such insights are impossible to obtain from analysing marketplaces or forums and need to be obtained from law enforcement. Academic studies looking at law enforcement agencies' responses to cybercrime are lacking, which merits more research is needed. Similarly, this can be argued for the financial and the security industry. These are also sectors in which similar quantitative approaches could lead to interesting insights into carding and other cybercrimes. Future research needs to explore these kinds of avenues.

The Web Science perspective used in this thesis made its focus, from an interdisciplinary perspective, wide-ranging. Whereas from a traditionally disciplinary perspective this could be seen as a limitation, this thesis has shown how insights from various disciplines can be used to extend on a method from a single discipline. An interdisciplinary perspective was regarded essential to understand the contextual factors and cognitive biases involved in carding. Technological advances in operational security of carders and other cybercriminals may make this research outdated. However, the importance of contextual factors and cognitive biases in the study of cybercrime will remain valid. Therefore, future research should continue to look at how these elements can lead to cybercriminals committing mistakes.

Ideally, decision-making of cybercriminals needs to be tested first-hand, by looking over their shoulders. However, such data is currently not available and would be hard to obtain, as researchers would have to engage in shadowing, i.e. looking over the shoulders of anonymous users Of course, such an ethnographic approach is complex to execute, because of ethical limitations and accessibility issues. Interviews with arrested cybercriminals, court documents or other detailed statements by (apprehended) carders could also inform future research looking into decision-making and modus operandi of cybercriminals.

It has been argued throughout this thesis that contextual factors and cognitive biases are important in understanding the decision-making of carders. It can be seen as a limitation of this thesis that these statements are not verified with statistical data. However, such data are hard to obtain. Experiments in ‘laboratory’ settings would be required to set-up such statistical tests. However, these would not be able to capture carders’ real-world decision-making under real risk. In future work, analyses of court documents on the operational security of carders and interviewees with carders can be used to provide statistical evidence on the prevalence of contextual factors and cognitive biases in the decision-making of cybercriminals. Comments by interviewees have also provided some evidence that law enforcement agencies’ and financial industry’s decision-making is also dependent on many contextual factors and cognitive biases. Future research could therefore also look into what factors affect their investigations. This could contribute to a better understanding of the motives of these parties and make them more aware of possible issues they will encounter in cooperation.

Appendix A

The agent model specifies the ‘people’ section of the *organisational aspects worksheet*. Tasks from the *task analysis worksheet* are also ascribed to agents here.

Agent model

Agent	Type
Name	Seller
Organisation	The seller determines the availability of stolen cards in the ‘organisation’, i.e. the forum or marketplace. These can help amplify the products of the seller to a wider audience than would otherwise be available. Also, contact with intermediaries that can make transactions safer can be established.
Involved in task	2, 4, 5, 7
Communicates with	Buyer; intermediary; moderator, administrator
Knowledge items	Forum, cryptocurrencies, (encrypted) messaging tools, Tor
Other competences	Escrow is not mentioned in tutorials, but is often demanded by the buyer to reduce the risk of scamming (Goldfeder et al., 2017; Yip, Shadbolt & Webber, 2013).
Responsibilities and constraints	**Responsibilities** - Make stolen card details available - Deliver card details - Appear trustworthy **Constraints** - Forum rules - Anti-carding efforts

Agent	Type
Name	Buyer
Organisation	The buyer is the driver of trade in stolen cards in the ‘organisation’, i.e. the forum or marketplace. The buyer uses these to establish contact with mainly vendors and intermediaries, and moderators if necessary. Also, buyers try to diminish the risk of being scammed by reading reviews of sellers. The value drivers mentioned in the Problem and opportunity worksheet help the buyer in

	engaging in safer transactions than when, for example, trading in person.
Involved in task	1, 2, 3, 6, 8, 9, 10, 11
Communicates with	Seller; intermediary; moderator, administrator
Knowledge items	Tutorials, Tor, forum, cryptocurrencies, Socks5, VPN, (encrypted) messaging tools, virtual machines, virtual encrypted disks, mac spoofing, Tor, remote desktop protocols, virtual private servers, drop addresses, postal addresses.
Other competences	Escrow is not mentioned in tutorials, but is used to reduce the scamming risk (Goldfeder et al., 2017; Yip, Shadbolt & Webber, 2013).
Responsibilities and constraints	**Responsibilities** - Staying anonymous - Paying for stolen cards - Making sure stolen cards still work - Making sure not to be scammed **Constraints** - Trusting anonymous sellers - Availability of cards

Agent	Type
Name	Intermediary (middleman, reviewer)
Organisation	The intermediary is active to increase trust in an anonymous environment. Vendors can send the intermediary cards to be checked and verified. Also, buyers can send them money, which the intermediary holds until the buyer confirms having received the cards from the seller. Intermediaries are also used as ‘packet mules’ when their houses are used to deliver packages.
Involved in task	2, 4, 7, 10. It must be noted that their involvement in tasks is generally optional. Buyers and sellers can also transact without intermediaries.
Communicates with	Buyer, seller
Knowledge items	Forum, Tor
Other competences	Escrow is not mentioned in the analysed tutorials, but it is an element for which intermediary agents are used. However, automated methods are gaining popularity (Horton-Eddison, 2017), which could make the demand for intermediaries, such as escrow facilitators, decrease. However, they could also offer automated escrow tools and charge a fee to the buyer and seller.
Responsibilities and constraints	**Responsibilities** - Appear trustworthy

	Constraints - Demand for technical intermediary (i.e. tools)

Agent	Type
Name	Moderator, administrator
Organisation	Moderators and administrators oversee the workings of their forum and/or marketplace and receive a percentage of every transaction for this. They often keep the user base informed on up-to-date vulnerabilities and security measures to take. Also, they resolve conflicts between buyers and sellers. They establish regulations for the usage of the forum/marketplace. If users are not acting according to the norms, moderators or administrators may ban them from using it.
Involved in	Not one specific task, but they may get involved in several parts of the process, such as 1, 5, 6 and 11.
Communicates with	Buyer, seller
Knowledge items	Forum, Tor, cryptocurrencies, (encrypted) messaging tools
Other competences	The ability to create understandable rules for the usage of the forum and/or marketplace. Also, the ability to deal fairly with conflicts between users and to remain trusted by user base.
Responsibilities and constraints	**Responsibilities** - Security of forum/marketplace and its users - Deal with conflicts - Appear neutral - Create forum rules **Constraints** - Law enforcement efforts - Technical vulnerabilities

Appendix B

Name	Role description	Institution	Anony-mous?	Years active in this area	Interview duration (minutes)	Country
Costel Ion	Digital Crime Officer in Research and Innovation	INTERPOL	No	15	47’	Romania
Brad Marden	Coordinator Investigation Support of Cybercrime Directorate	INTERPOL	No	12	33’	Aus-tralian
Roeland van Zeijst	Digital crime officer in Strategy and Outreach	INTERPOL	No	5	52’	Dutch
Maarten Jak	(Cybercrime) Intelligence Specialist	ABN AMRO	No	4	38’	Dutch
Rob Heijjer	Senior Advisor Financial Economic Crime	Rabobank	No	10+	1h11	Dutch
Niels Ploeger	Strategic account manager	Anti-Money Laundering Centre	No	10	1h22 (three-person interview)	Dutch
Johan van Wilsem	Head of the Department of Crime, Law Enforcement	WODC	No	9	40’	Dutch

	and Sanctions at Research and Documentation Centre (WODC), Dutch Ministry of Security and Justice					
Anonymous	Financial detective	Dutch national financial crime unit	Yes	15+	1h22 (three-person interview)	Dutch
Anonymous	Financial detective	Team High Tech Crime	Yes	5+	1h22 (three-person interview)	Dutch
Anonymous	Policy advisor	Dutch public prosecution service	Yes	3	42’ (two-person interview)	Dutch
Anonymous	Operational analyst	Dutch National Police	Yes	20+	42’ (two-person interview)	Dutch
Anonymous	Seconded National Expert	Europol	Yes	15+	1h00	Italian
Anonymous	Operational specialist	Dutch National Police	Yes	4	30’	Dutch
Anonymous	Operational specialist	Dutch National Police	Yes	6	51’	Dutch
Anonymous	Digital Crime	INTERPOL	Yes	6	30’	Aus-

	Officer					tralian
Anonymous	Investigations manager	Card issuer	Yes	12	1h05 (two-person interview)	Dutch
Anonymous	Investigator	Card issuer	Yes	9	1h05 (two-person interview)	Dutch
Anonymous	Police officer	International organisation	Yes	6	45’	“West-African”
Anonymous	Investigator Operational Fraud	Payment service provider	Yes	20	1h43	Dutch

Table B.1 Randomised list of interviewees

Appendix C

Background of interviewee

- Can you describe your current role?
- How long have you been working in this industry?

Carding

- How big of a problem is carding (online card fraud) for your organisation (or country)?
- What effort is put into tackling the issue of carding in your organisation?
- Is this an adequate response compared to the size of the problem?
- If not, what do you think could/should change?

Tools and operational security

- What tools do you think carders mainly use in cashing out stolen payment cards?
- What do you think the weakest links are in the OPSEC of carders?
- Are there common mistakes that are made over and over again? Can you describe them for me?
- Why do you think these mistakes are made?
- What level of deviation from using these tools is necessary (if any), before a case can be pursued/prosecuted?
- Does less operational security mean more arrests? Or does the number of arrests also depend on other factors?

Measures to take

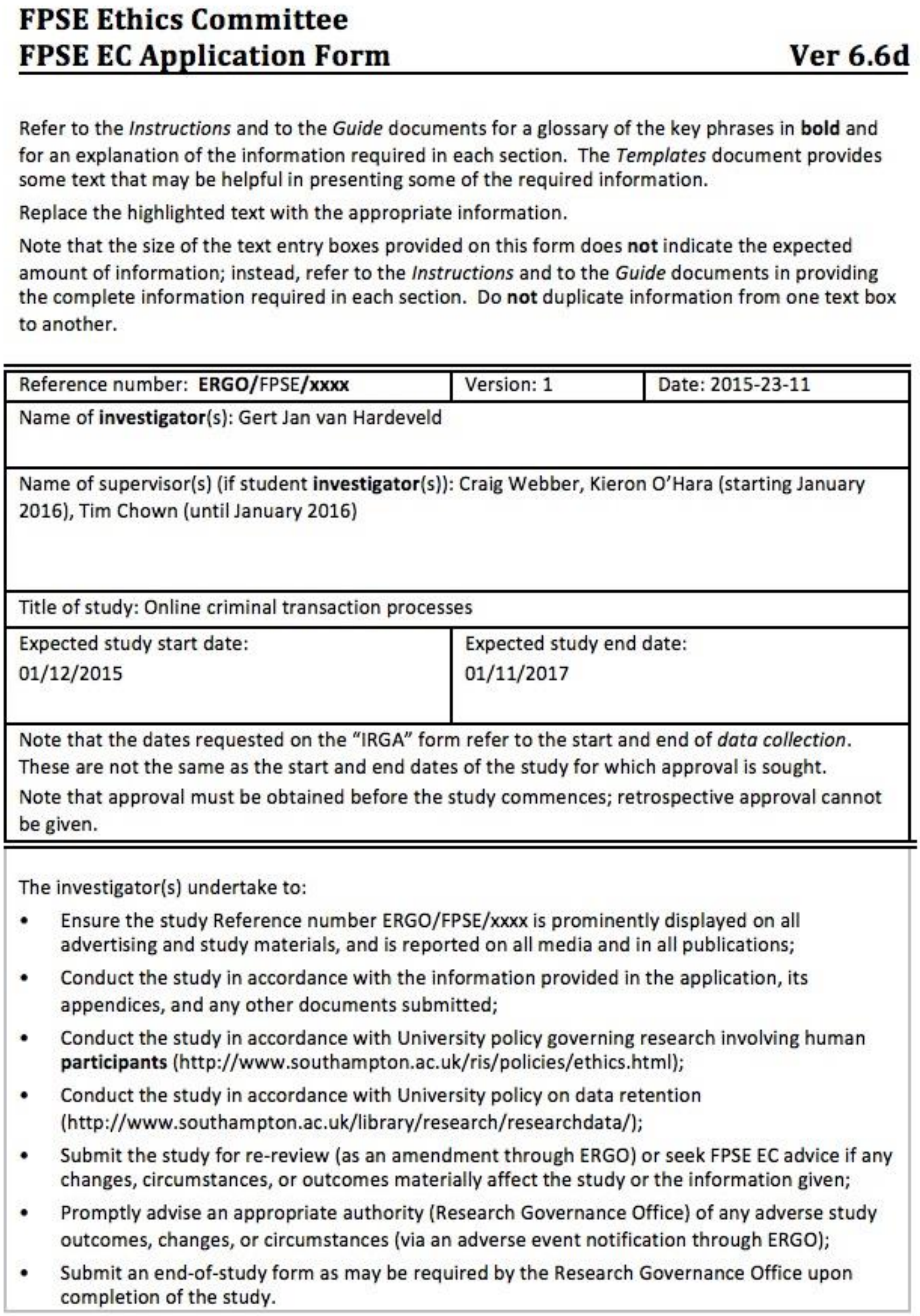
- Can operational security mistakes be exploited?

- What measures are currently taken in regards to operational security mistakes?
- What kind of approach is needed to minimise (the efficiency of) carding?
- What are the main barriers in addressing the issue of carding?
- What are the financial and resource limitations? How do you decide which crimes to prosecute?

What happens after?

- What do you think will happen if you implement your measures?

Appendix D



FPSE Ethics Committee

FPSE EC Application Form **Ver 6.6d**

Refer to the *Instructions* and to the *Guide* documents for a glossary of the key phrases in **bold** and for an explanation of the information required in each section. The *Templates* document provides some text that may be helpful in presenting some of the required information.

Replace the highlighted text with the appropriate information.

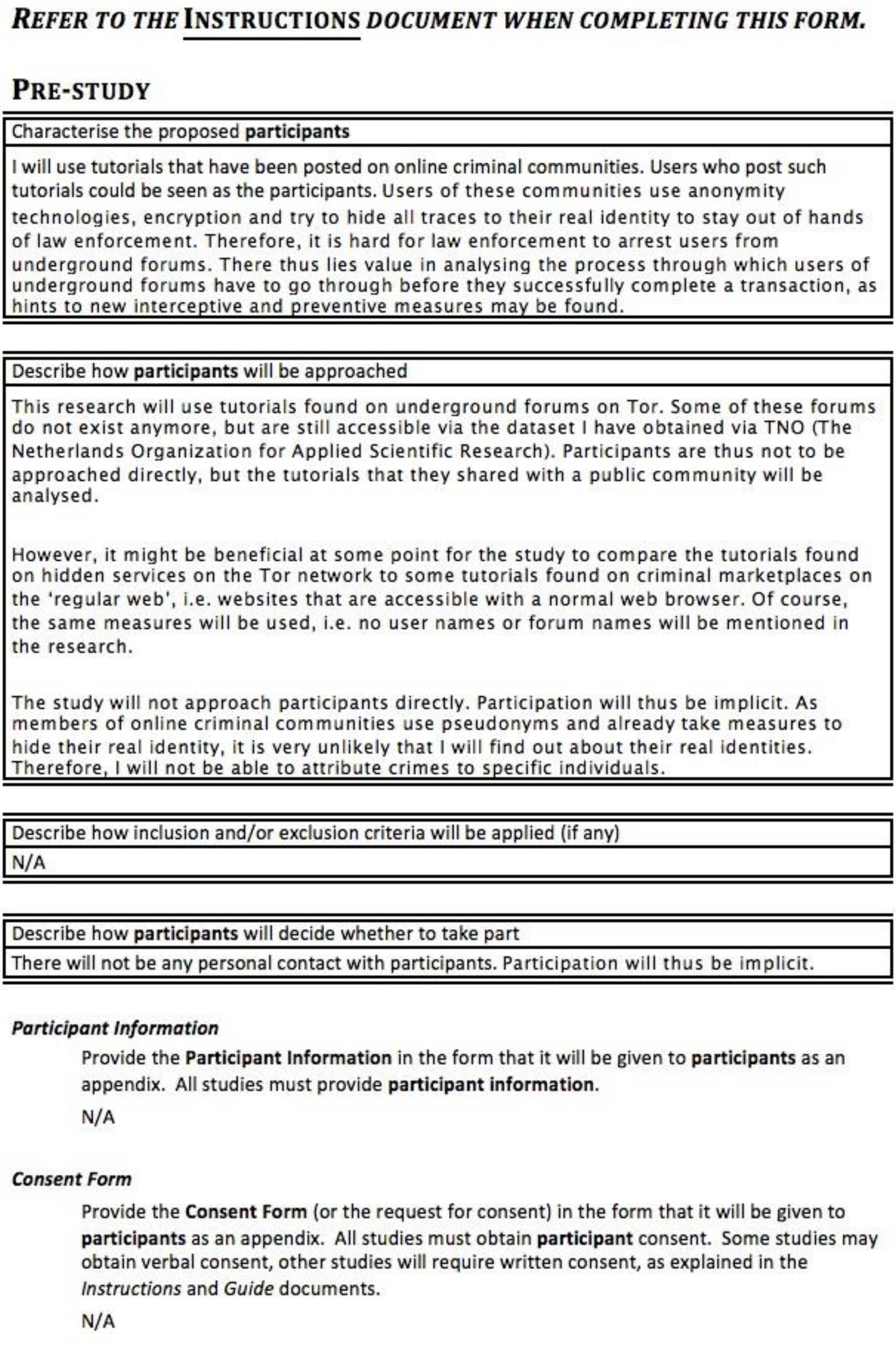
Note that the size of the text entry boxes provided on this form does **not** indicate the expected amount of information; instead, refer to the *Instructions* and to the *Guide* documents in providing the complete information required in each section. Do **not** duplicate information from one text box to another.

Reference number: **ERGO/**FPSE**/xxxx**	Version: 1	Date: 2015-23-11
Name of **investigator**(s): Gert Jan van Hardeveld		
Name of supervisor(s) (if student **investigator**(s)): Craig Webber, Kieron O'Hara (starting January 2016), Tim Chown (until January 2016)		
Title of study: Online criminal transaction processes		
Expected study start date: 01/12/2015	Expected study end date: 01/11/2017	
Note that the dates requested on the "IRGA" form refer to the start and end of *data collection*. These are not the same as the start and end dates of the study for which approval is sought. Note that approval must be obtained before the study commences; retrospective approval cannot be given.		

The investigator(s) undertake to:

- Ensure the study Reference number ERGO/FPSE/xxxx is prominently displayed on all advertising and study materials, and is reported on all media and in all publications;
- Conduct the study in accordance with the information provided in the application, its appendices, and any other documents submitted;
- Conduct the study in accordance with University policy governing research involving human **participants** (http://www.southampton.ac.uk/ris/policies/ethics.html);
- Conduct the study in accordance with University policy on data retention (http://www.southampton.ac.uk/library/research/researchdata/);
- Submit the study for re-review (as an amendment through ERGO) or seek FPSE EC advice if any changes, circumstances, or outcomes materially affect the study or the information given;
- Promptly advise an appropriate authority (Research Governance Office) of any adverse study outcomes, changes, or circumstances (via an adverse event notification through ERGO);
- Submit an end-of-study form as may be required by the Research Governance Office upon completion of the study.

Appendix D



REFER TO THE* <u>INSTRUCTIONS</u> *DOCUMENT WHEN COMPLETING THIS FORM.

PRE-STUDY

Characterise the proposed **participants**
I will use tutorials that have been posted on online criminal communities. Users who post such tutorials could be seen as the participants. Users of these communities use anonymity technologies, encryption and try to hide all traces to their real identity to stay out of hands of law enforcement. Therefore, it is hard for law enforcement to arrest users from underground forums. There thus lies value in analysing the process through which users of underground forums have to go through before they successfully complete a transaction, as hints to new interceptive and preventive measures may be found.

Describe how **participants** will be approached
This research will use tutorials found on underground forums on Tor. Some of these forums do not exist anymore, but are still accessible via the dataset I have obtained via TNO (The Netherlands Organization for Applied Scientific Research). Participants are thus not to be approached directly, but the tutorials that they shared with a public community will be analysed. However, it might be beneficial at some point for the study to compare the tutorials found on hidden services on the Tor network to some tutorials found on criminal marketplaces on the 'regular web', i.e. websites that are accessible with a normal web browser. Of course, the same measures will be used, i.e. no user names or forum names will be mentioned in the research. The study will not approach participants directly. Participation will thus be implicit. As members of online criminal communities use pseudonyms and already take measures to hide their real identity, it is very unlikely that I will find out about their real identities. Therefore, I will not be able to attribute crimes to specific individuals.

Describe how inclusion and/or exclusion criteria will be applied (if any)
N/A

Describe how **participants** will decide whether to take part
There will not be any personal contact with participants. Participation will thus be implicit.

Participant Information

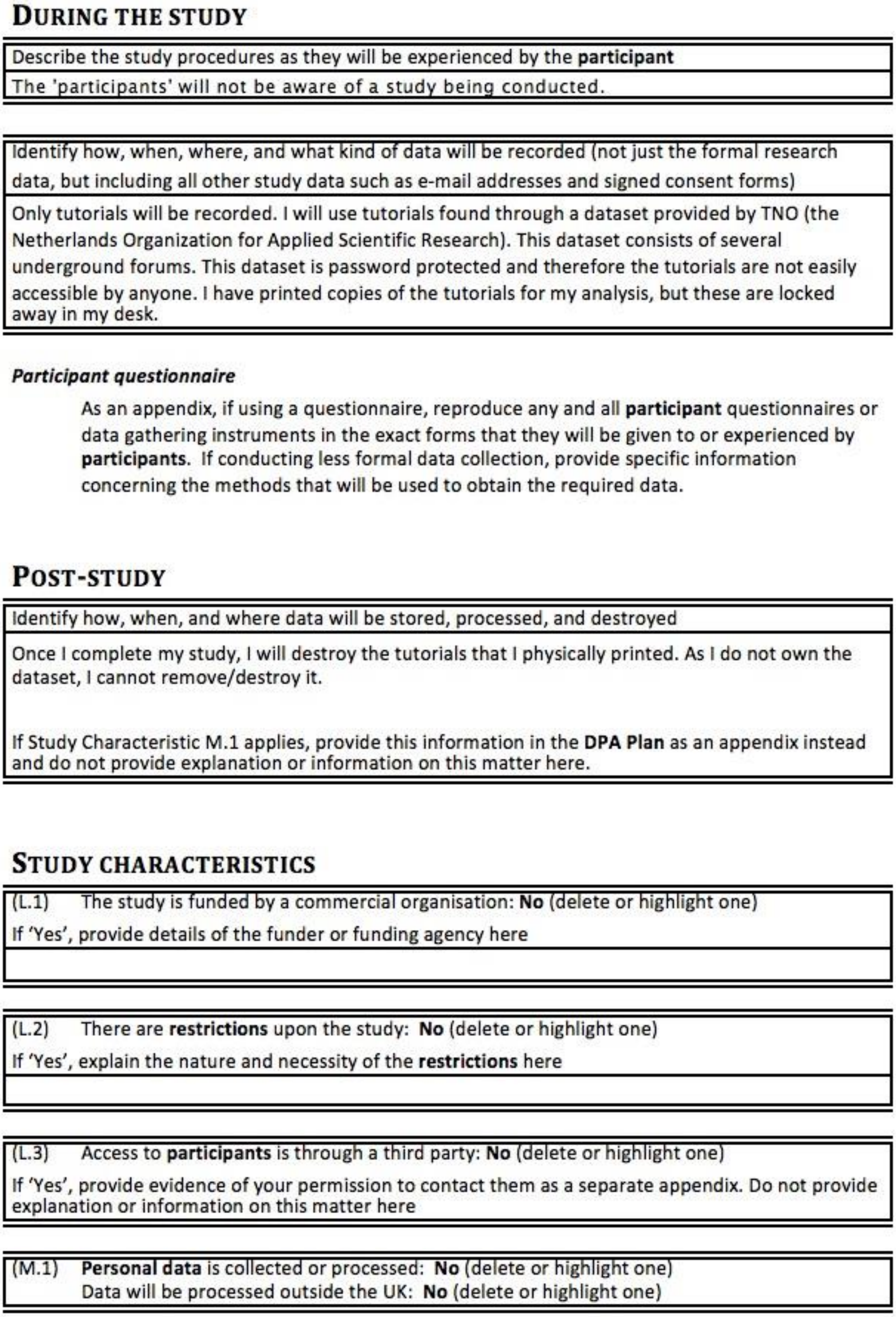
Provide the **Participant Information** in the form that it will be given to **participants** as an appendix. All studies must provide **participant information**.

N/A

Consent Form

Provide the **Consent Form** (or the request for consent) in the form that it will be given to **participants** as an appendix. All studies must obtain **participant** consent. Some studies may obtain verbal consent, other studies will require written consent, as explained in the *Instructions* and *Guide* documents.

N/A



During the study

Describe the study procedures as they will be experienced by the **participant**
The 'participants' will not be aware of a study being conducted.

Identify how, when, where, and what kind of data will be recorded (not just the formal research data, but including all other study data such as e-mail addresses and signed consent forms)
Only tutorials will be recorded. I will use tutorials found through a dataset provided by TNO (the Netherlands Organization for Applied Scientific Research). This dataset consists of several underground forums. This dataset is password protected and therefore the tutorials are not easily accessible by anyone. I have printed copies of the tutorials for my analysis, but these are locked away in my desk.

Participant questionnaire

As an appendix, if using a questionnaire, reproduce any and all **participant** questionnaires or data gathering instruments in the exact forms that they will be given to or experienced by **participants**. If conducting less formal data collection, provide specific information concerning the methods that will be used to obtain the required data.

Post-study

Identify how, when, and where data will be stored, processed, and destroyed
Once I complete my study, I will destroy the tutorials that I physically printed. As I do not own the dataset, I cannot remove/destroy it. If Study Characteristic M.1 applies, provide this information in the **DPA Plan** as an appendix instead and do not provide explanation or information on this matter here.

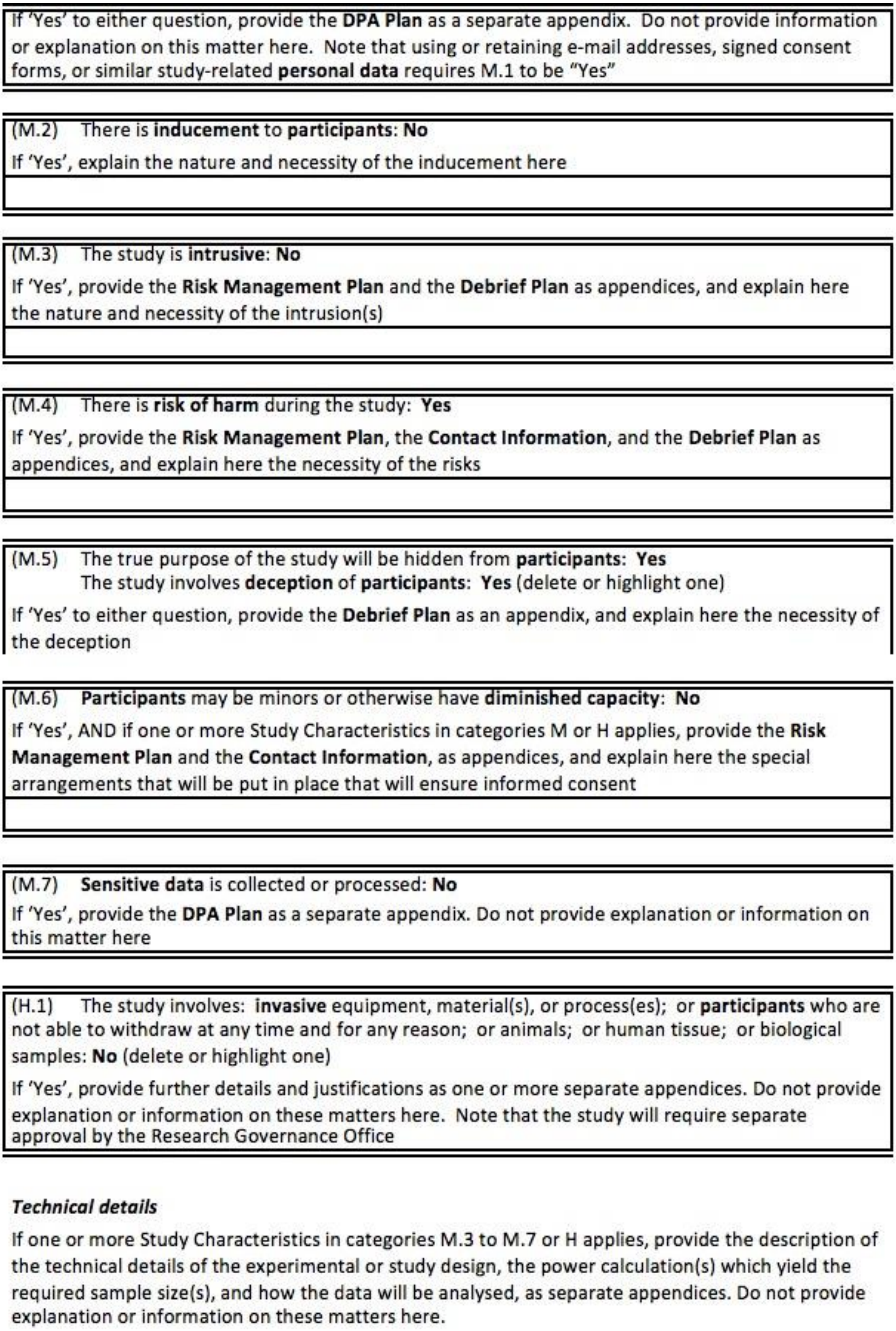
Study characteristics

(L.1) The study is funded by a commercial organisation: **No** (delete or highlight one) If 'Yes', provide details of the funder or funding agency here

(L.2) There are **restrictions** upon the study: **No** (delete or highlight one) If 'Yes', explain the nature and necessity of the **restrictions** here

(L.3) Access to **participants** is through a third party: **No** (delete or highlight one) If 'Yes', provide evidence of your permission to contact them as a separate appendix. Do not provide explanation or information on this matter here

(M.1) **Personal data** is collected or processed: **No** (delete or highlight one) Data will be processed outside the UK: **No** (delete or highlight one)



If 'Yes' to either question, provide the **DPA Plan** as a separate appendix. Do not provide information or explanation on this matter here. Note that using or retaining e-mail addresses, signed consent forms, or similar study-related **personal data** requires M.1 to be "Yes"

(M.2) There is **inducement** to **participants**: **No**

If 'Yes', explain the nature and necessity of the inducement here

(M.3) The study is **intrusive**: **No**

If 'Yes', provide the **Risk Management Plan** and the **Debrief Plan** as appendices, and explain here the nature and necessity of the intrusion(s)

(M.4) There is **risk of harm** during the study: **Yes**

If 'Yes', provide the **Risk Management Plan**, the **Contact Information**, and the **Debrief Plan** as appendices, and explain here the necessity of the risks

(M.5) The true purpose of the study will be hidden from **participants**: **Yes**
The study involves **deception** of **participants**: **Yes** (delete or highlight one)

If 'Yes' to either question, provide the **Debrief Plan** as an appendix, and explain here the necessity of the deception

(M.6) **Participants** may be minors or otherwise have **diminished capacity**: **No**

If 'Yes', AND if one or more Study Characteristics in categories M or H applies, provide the **Risk Management Plan** and the **Contact Information**, as appendices, and explain here the special arrangements that will be put in place that will ensure informed consent

(M.7) **Sensitive data** is collected or processed: **No**

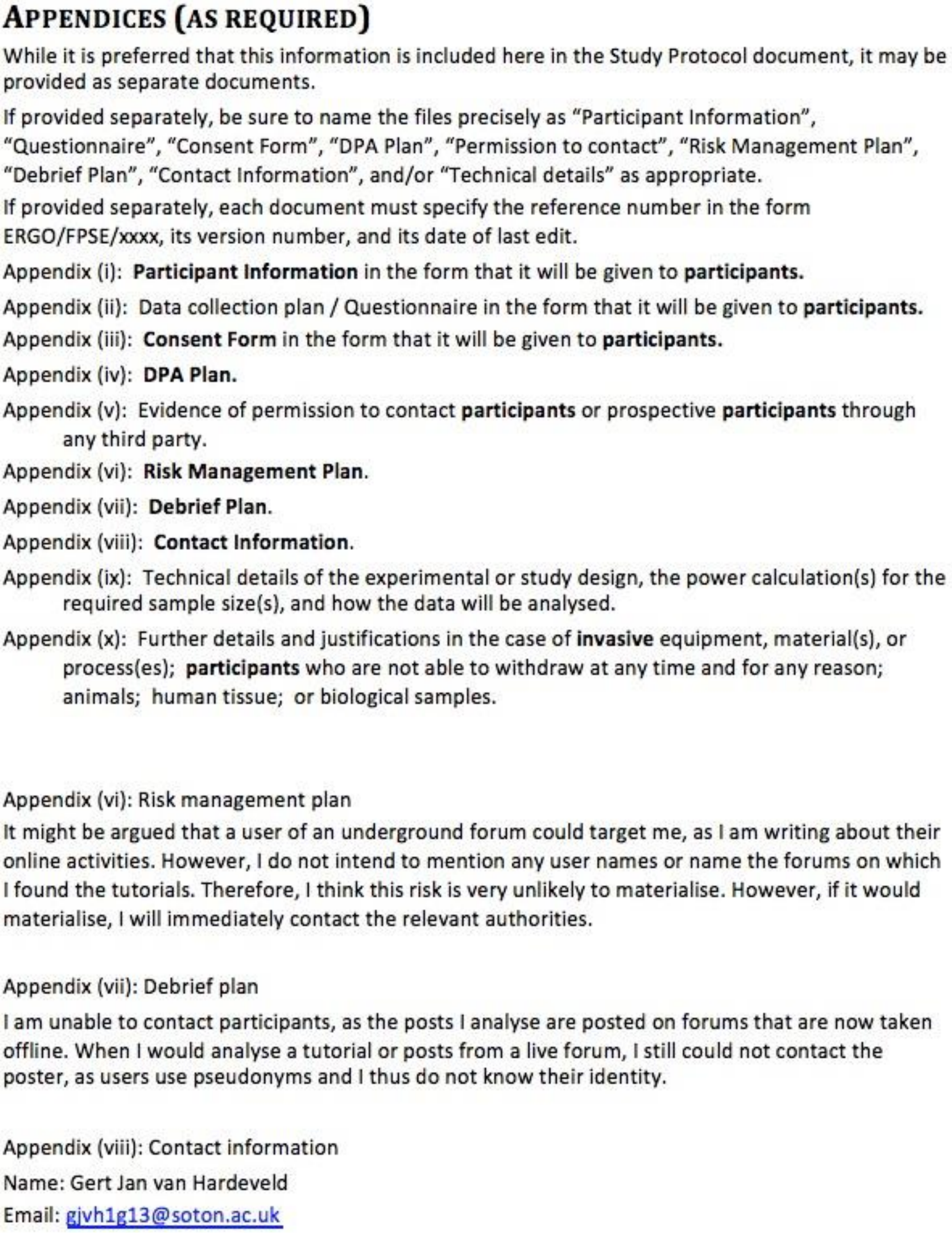
If 'Yes', provide the **DPA Plan** as a separate appendix. Do not provide explanation or information on this matter here

(H.1) The study involves: **invasive** equipment, material(s), or process(es); or **participants** who are not able to withdraw at any time and for any reason; or animals; or human tissue; or biological samples: **No** (delete or highlight one)

If 'Yes', provide further details and justifications as one or more separate appendices. Do not provide explanation or information on these matters here. Note that the study will require separate approval by the Research Governance Office

Technical details

If one or more Study Characteristics in categories M.3 to M.7 or H applies, provide the description of the technical details of the experimental or study design, the power calculation(s) which yield the required sample size(s), and how the data will be analysed, as separate appendices. Do not provide explanation or information on these matters here.



APPENDICES (AS REQUIRED)

While it is preferred that this information is included here in the Study Protocol document, it may be provided as separate documents.

If provided separately, be sure to name the files precisely as "Participant Information", "Questionnaire", "Consent Form", "DPA Plan", "Permission to contact", "Risk Management Plan", "Debrief Plan", "Contact Information", and/or "Technical details" as appropriate.

If provided separately, each document must specify the reference number in the form ERGO/FPSE/xxxx, its version number, and its date of last edit.

Appendix (i): **Participant Information** in the form that it will be given to **participants.**

Appendix (ii): Data collection plan / Questionnaire in the form that it will be given to **participants.**

Appendix (iii): **Consent Form** in the form that it will be given to **participants.**

Appendix (iv): **DPA Plan.**

Appendix (v): Evidence of permission to contact **participants** or prospective **participants** through any third party.

Appendix (vi): **Risk Management Plan**.

Appendix (vii): **Debrief Plan**.

Appendix (viii): **Contact Information**.

Appendix (ix): Technical details of the experimental or study design, the power calculation(s) for the required sample size(s), and how the data will be analysed.

Appendix (x): Further details and justifications in the case of **invasive** equipment, material(s), or process(es); **participants** who are not able to withdraw at any time and for any reason; animals; human tissue; or biological samples.

Appendix (vi): Risk management plan

It might be argued that a user of an underground forum could target me, as I am writing about their online activities. However, I do not intend to mention any user names or name the forums on which I found the tutorials. Therefore, I think this risk is very unlikely to materialise. However, if it would materialise, I will immediately contact the relevant authorities.

Appendix (vii): Debrief plan

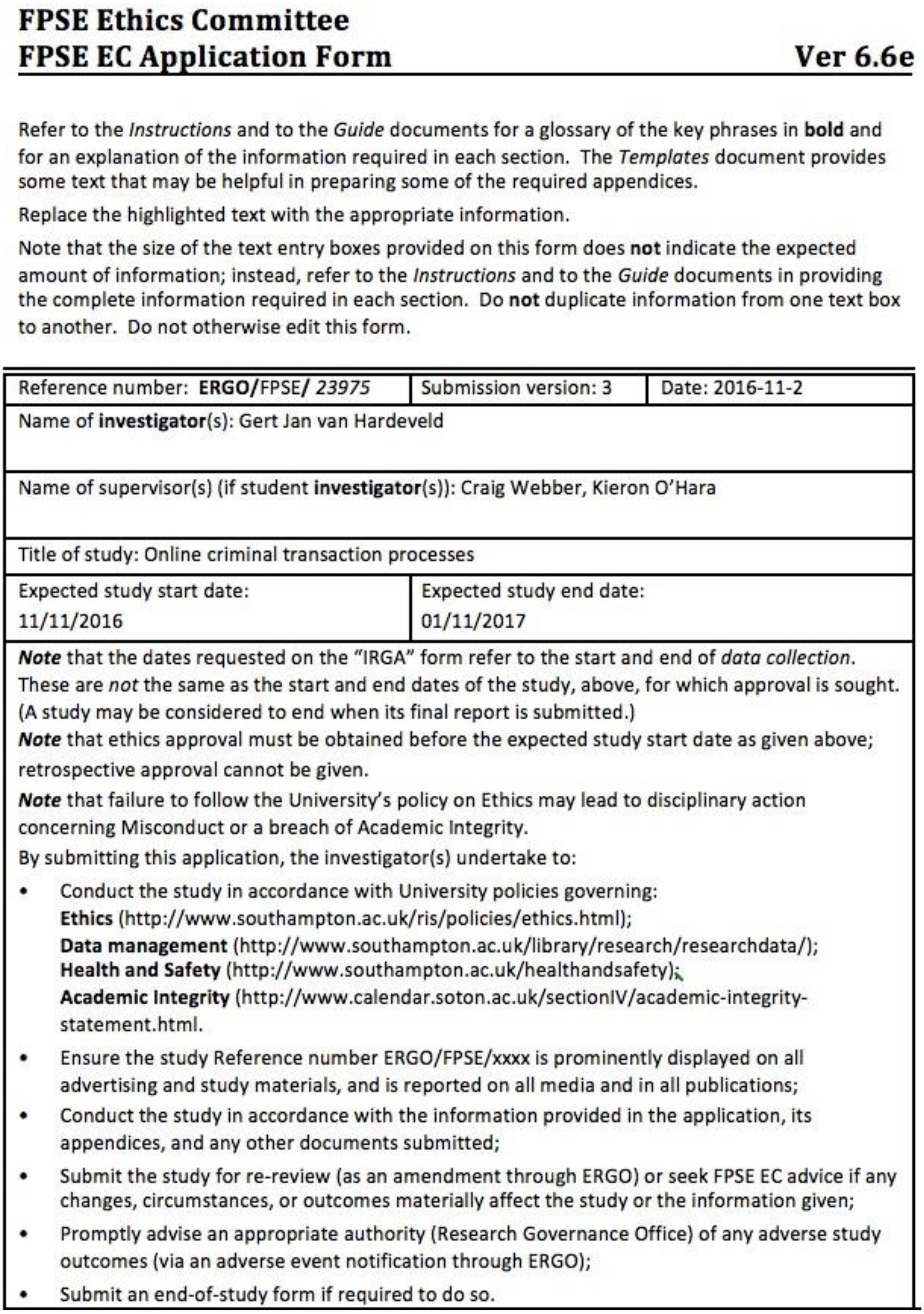
I am unable to contact participants, as the posts I analyse are posted on forums that are now taken offline. When I would analyse a tutorial or posts from a live forum, I still could not contact the poster, as users use pseudonyms and I thus do not know their identity.

Appendix (viii): Contact information

Name: Gert Jan van Hardeveld

Email: gjvh1g13@soton.ac.uk

Appendix E



FPSE Ethics Committee
FPSE EC Application Form Ver 6.6e

Refer to the *Instructions* and to the *Guide* documents for a glossary of the key phrases in **bold** and for an explanation of the information required in each section. The *Templates* document provides some text that may be helpful in preparing some of the required appendices.

Replace the highlighted text with the appropriate information.

Note that the size of the text entry boxes provided on this form does **not** indicate the expected amount of information; instead, refer to the *Instructions* and to the *Guide* documents in providing the complete information required in each section. Do **not** duplicate information from one text box to another. Do not otherwise edit this form.

Reference number: **ERGO/**FPSE**/** *23975*	Submission version: 3	Date: 2016-11-2

Name of **investigator**(s): Gert Jan van Hardeveld

Name of supervisor(s) (if student **investigator**(s)): Craig Webber, Kieron O'Hara

Title of study: Online criminal transaction processes

Expected study start date: 11/11/2016	Expected study end date: 01/11/2017

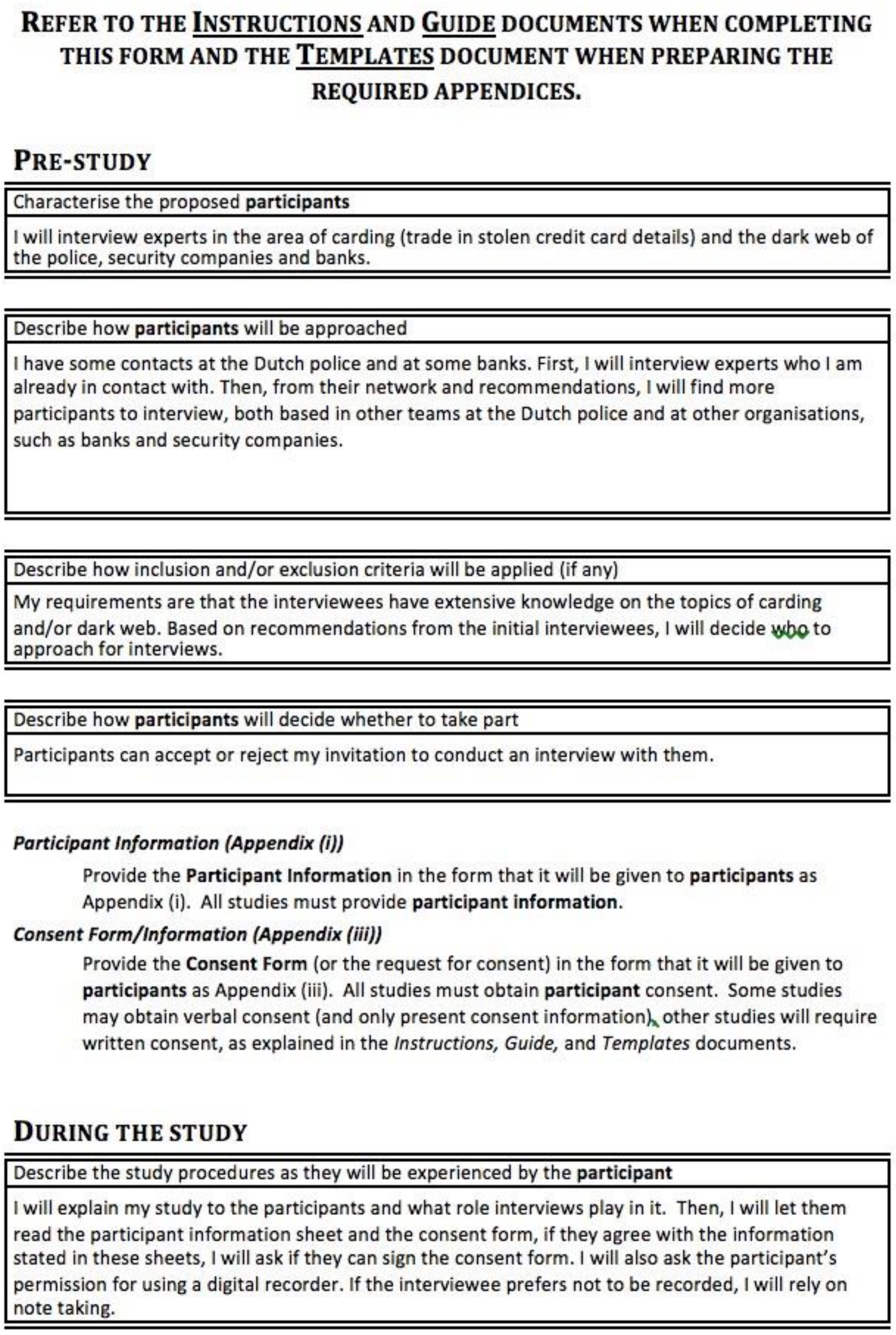
Note that the dates requested on the "IRGA" form refer to the start and end of *data collection*. These are *not* the same as the start and end dates of the study, above, for which approval is sought. (A study may be considered to end when its final report is submitted.)

Note that ethics approval must be obtained before the expected study start date as given above; retrospective approval cannot be given.

Note that failure to follow the University's policy on Ethics may lead to disciplinary action concerning Misconduct or a breach of Academic Integrity.

By submitting this application, the investigator(s) undertake to:

- Conduct the study in accordance with University policies governing:
  Ethics (http://www.southampton.ac.uk/ris/policies/ethics.html);
  Data management (http://www.southampton.ac.uk/library/research/researchdata/);
  Health and Safety (http://www.southampton.ac.uk/healthandsafety);
  Academic Integrity (http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-statement.html.
- Ensure the study Reference number ERGO/FPSE/xxxx is prominently displayed on all advertising and study materials, and is reported on all media and in all publications;
- Conduct the study in accordance with the information provided in the application, its appendices, and any other documents submitted;
- Submit the study for re-review (as an amendment through ERGO) or seek FPSE EC advice if any changes, circumstances, or outcomes materially affect the study or the information given;
- Promptly advise an appropriate authority (Research Governance Office) of any adverse study outcomes (via an adverse event notification through ERGO);
- Submit an end-of-study form if required to do so.



REFER TO THE INSTRUCTIONS AND GUIDE DOCUMENTS WHEN COMPLETING THIS FORM AND THE TEMPLATES DOCUMENT WHEN PREPARING THE REQUIRED APPENDICES.

PRE-STUDY

Characterise the proposed **participants**
I will interview experts in the area of carding (trade in stolen credit card details) and the dark web of the police, security companies and banks.

Describe how **participants** will be approached
I have some contacts at the Dutch police and at some banks. First, I will interview experts who I am already in contact with. Then, from their network and recommendations, I will find more participants to interview, both based in other teams at the Dutch police and at other organisations, such as banks and security companies.

Describe how inclusion and/or exclusion criteria will be applied (if any)
My requirements are that the interviewees have extensive knowledge on the topics of carding and/or dark web. Based on recommendations from the initial interviewees, I will decide who to approach for interviews.

Describe how **participants** will decide whether to take part
Participants can accept or reject my invitation to conduct an interview with them.

Participant Information (Appendix (i))

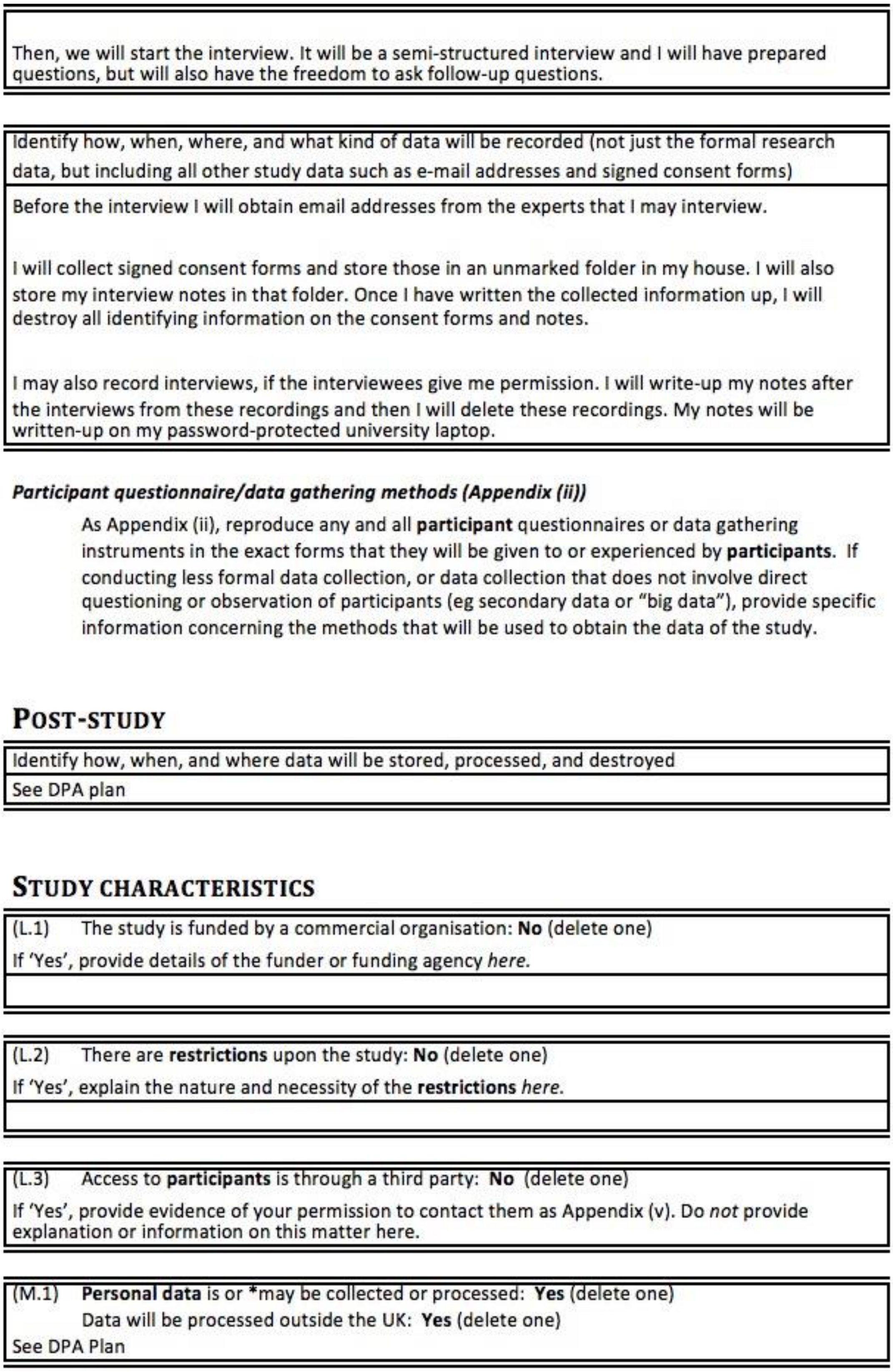
Provide the **Participant Information** in the form that it will be given to **participants** as Appendix (i). All studies must provide **participant information**.

Consent Form/Information (Appendix (iii))

Provide the **Consent Form** (or the request for consent) in the form that it will be given to **participants** as Appendix (iii). All studies must obtain **participant** consent. Some studies may obtain verbal consent (and only present consent information), other studies will require written consent, as explained in the *Instructions, Guide,* and *Templates* documents.

DURING THE STUDY

Describe the study procedures as they will be experienced by the **participant**
I will explain my study to the participants and what role interviews play in it. Then, I will let them read the participant information sheet and the consent form, if they agree with the information stated in these sheets, I will ask if they can sign the consent form. I will also ask the participant's permission for using a digital recorder. If the interviewee prefers not to be recorded, I will rely on note taking.



Then, we will start the interview. It will be a semi-structured interview and I will have prepared questions, but will also have the freedom to ask follow-up questions.

Identify how, when, where, and what kind of data will be recorded (not just the formal research data, but including all other study data such as e-mail addresses and signed consent forms)

Before the interview I will obtain email addresses from the experts that I may interview.

I will collect signed consent forms and store those in an unmarked folder in my house. I will also store my interview notes in that folder. Once I have written the collected information up, I will destroy all identifying information on the consent forms and notes.

I may also record interviews, if the interviewees give me permission. I will write-up my notes after the interviews from these recordings and then I will delete these recordings. My notes will be written-up on my password-protected university laptop.

Participant questionnaire/data gathering methods (Appendix (ii))

As Appendix (ii), reproduce any and all **participant** questionnaires or data gathering instruments in the exact forms that they will be given to or experienced by **participants**. If conducting less formal data collection, or data collection that does not involve direct questioning or observation of participants (eg secondary data or "big data"), provide specific information concerning the methods that will be used to obtain the data of the study.

POST-STUDY

Identify how, when, and where data will be stored, processed, and destroyed

See DPA plan

STUDY CHARACTERISTICS

(L.1) The study is funded by a commercial organisation: **No** (delete one)

If 'Yes', provide details of the funder or funding agency *here.*

(L.2) There are **restrictions** upon the study: **No** (delete one)

If 'Yes', explain the nature and necessity of the **restrictions** *here.*

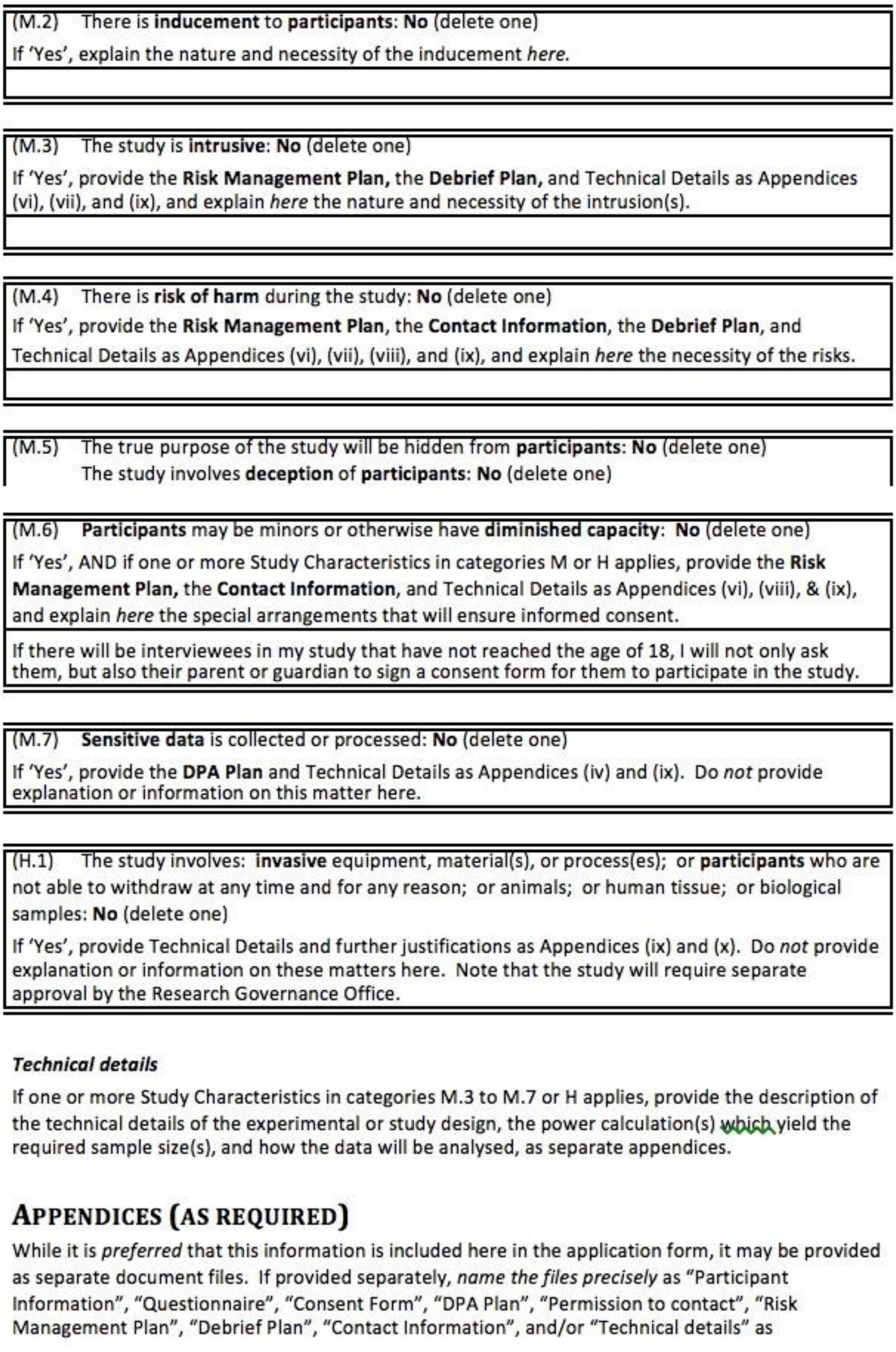
(L.3) Access to **participants** is through a third party: **No** (delete one)

If 'Yes', provide evidence of your permission to contact them as Appendix (v). Do *not* provide explanation or information on this matter here.

(M.1) **Personal data** is or *may be collected or processed: **Yes** (delete one)

Data will be processed outside the UK: **Yes** (delete one)

See DPA Plan



(M.2) There is **inducement** to **participants**: **No** (delete one)

If 'Yes', explain the nature and necessity of the inducement *here.*

(M.3) The study is **intrusive**: **No** (delete one)

If 'Yes', provide the **Risk Management Plan,** the **Debrief Plan,** and Technical Details as Appendices (vi), (vii), and (ix), and explain *here* the nature and necessity of the intrusion(s).

(M.4) There is **risk of harm** during the study: **No** (delete one)

If 'Yes', provide the **Risk Management Plan**, the **Contact Information**, the **Debrief Plan**, and Technical Details as Appendices (vi), (vii), (viii), and (ix), and explain *here* the necessity of the risks.

(M.5) The true purpose of the study will be hidden from **participants**: **No** (delete one)
The study involves **deception** of **participants**: **No** (delete one)

(M.6) **Participants** may be minors or otherwise have **diminished capacity**: **No** (delete one)

If 'Yes', AND if one or more Study Characteristics in categories M or H applies, provide the **Risk Management Plan,** the **Contact Information**, and Technical Details as Appendices (vi), (viii), & (ix), and explain *here* the special arrangements that will ensure informed consent.

If there will be interviewees in my study that have not reached the age of 18, I will not only ask them, but also their parent or guardian to sign a consent form for them to participate in the study.

(M.7) **Sensitive data** is collected or processed: **No** (delete one)

If 'Yes', provide the **DPA Plan** and Technical Details as Appendices (iv) and (ix). Do *not* provide explanation or information on this matter here.

(H.1) The study involves: **invasive** equipment, material(s), or process(es); or **participants** who are not able to withdraw at any time and for any reason; or animals; or human tissue; or biological samples: **No** (delete one)

If 'Yes', provide Technical Details and further justifications as Appendices (ix) and (x). Do *not* provide explanation or information on these matters here. Note that the study will require separate approval by the Research Governance Office.

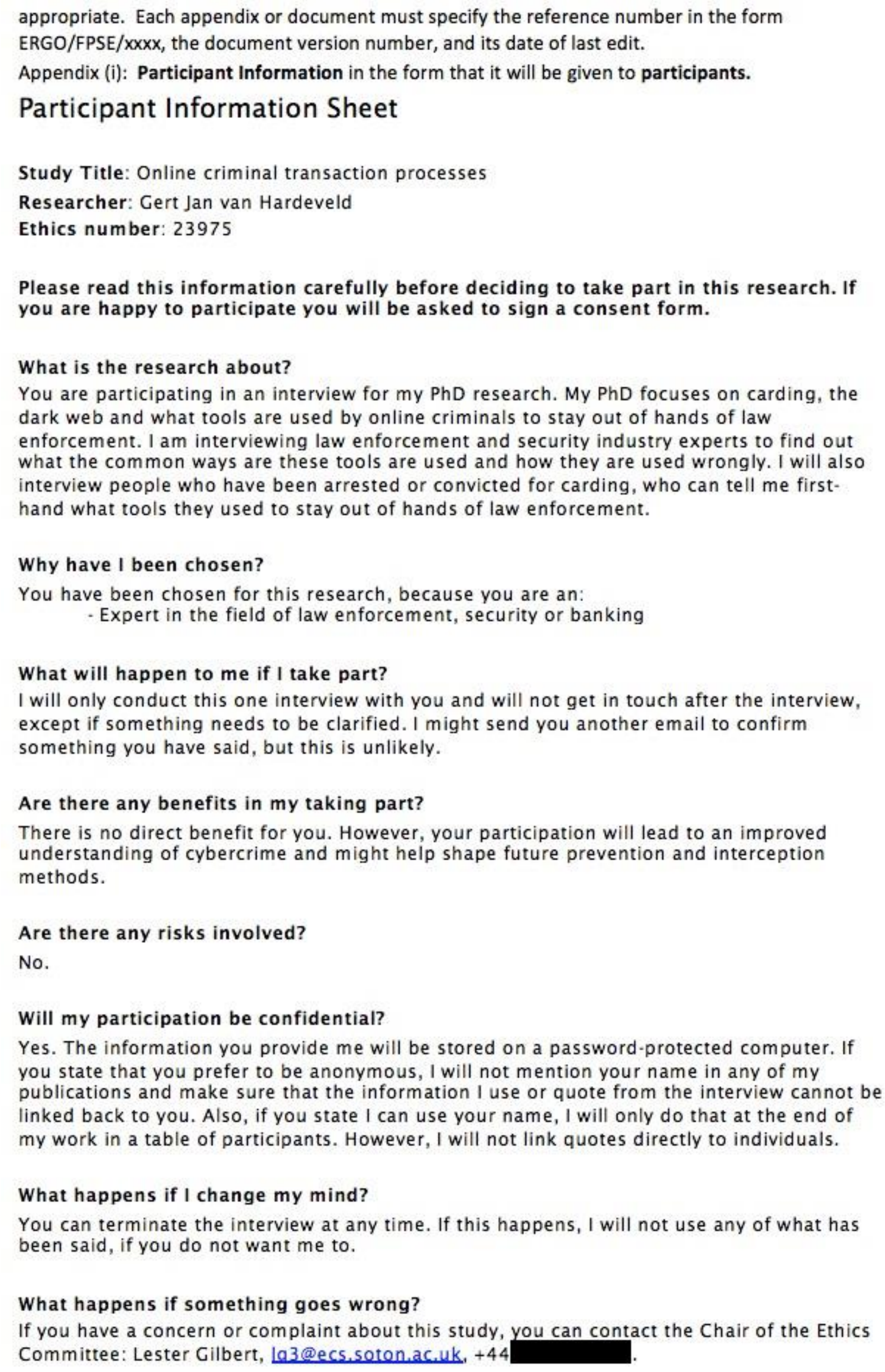
Technical details

If one or more Study Characteristics in categories M.3 to M.7 or H applies, provide the description of the technical details of the experimental or study design, the power calculation(s) which yield the required sample size(s), and how the data will be analysed, as separate appendices.

Appendices (as required)

While it is *preferred* that this information is included here in the application form, it may be provided as separate document files. If provided separately, *name the files precisely* as "Participant Information", "Questionnaire", "Consent Form", "DPA Plan", "Permission to contact", "Risk Management Plan", "Debrief Plan", "Contact Information", and/or "Technical details" as

Appendix E



appropriate. Each appendix or document must specify the reference number in the form ERGO/FPSE/xxxx, the document version number, and its date of last edit.

Appendix (i): **Participant Information** in the form that it will be given to **participants.**

Participant Information Sheet

Study Title: Online criminal transaction processes

Researcher: Gert Jan van Hardeveld

Ethics number: 23975

Please read this information carefully before deciding to take part in this research. If you are happy to participate you will be asked to sign a consent form.

What is the research about?

You are participating in an interview for my PhD research. My PhD focuses on carding, the dark web and what tools are used by online criminals to stay out of hands of law enforcement. I am interviewing law enforcement and security industry experts to find out what the common ways are these tools are used and how they are used wrongly. I will also interview people who have been arrested or convicted for carding, who can tell me first-hand what tools they used to stay out of hands of law enforcement.

Why have I been chosen?

You have been chosen for this research, because you are an:

- Expert in the field of law enforcement, security or banking

What will happen to me if I take part?

I will only conduct this one interview with you and will not get in touch after the interview, except if something needs to be clarified. I might send you another email to confirm something you have said, but this is unlikely.

Are there any benefits in my taking part?

There is no direct benefit for you. However, your participation will lead to an improved understanding of cybercrime and might help shape future prevention and interception methods.

Are there any risks involved?

No.

Will my participation be confidential?

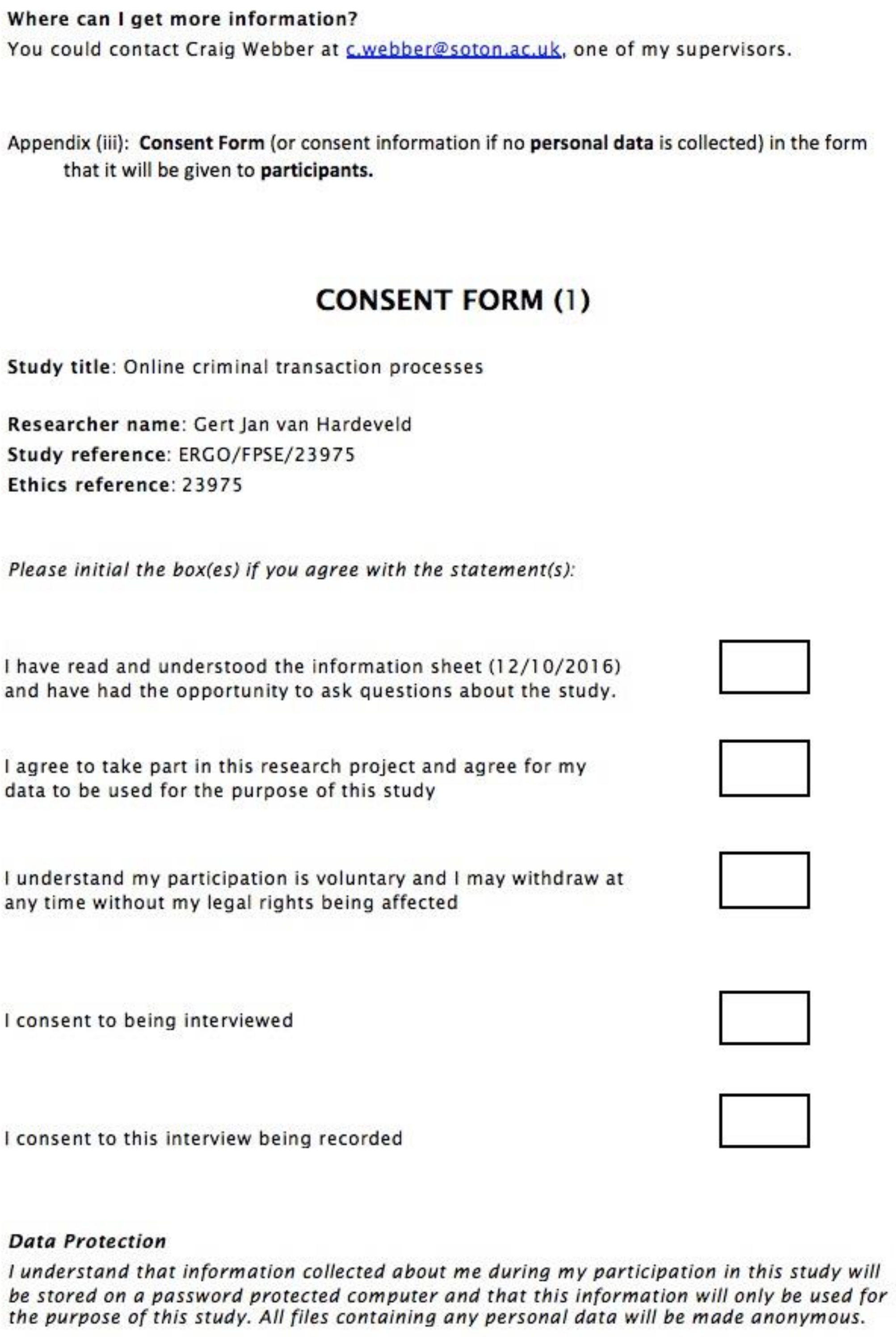
Yes. The information you provide me will be stored on a password-protected computer. If you state that you prefer to be anonymous, I will not mention your name in any of my publications and make sure that the information I use or quote from the interview cannot be linked back to you. Also, if you state I can use your name, I will only do that at the end of my work in a table of participants. However, I will not link quotes directly to individuals.

What happens if I change my mind?

You can terminate the interview at any time. If this happens, I will not use any of what has been said, if you do not want me to.

What happens if something goes wrong?

If you have a concern or complaint about this study, you can contact the Chair of the Ethics Committee: Lester Gilbert, lg3@ecs.soton.ac.uk, +44[redacted].



Where can I get more information?

You could contact Craig Webber at c.webber@soton.ac.uk, one of my supervisors.

Appendix (iii): **Consent Form** (or consent information if no **personal data** is collected) in the form that it will be given to **participants.**

CONSENT FORM (1)

Study title: Online criminal transaction processes

Researcher name: Gert Jan van Hardeveld
Study reference: ERGO/FPSE/23975
Ethics reference: 23975

Please initial the box(es) if you agree with the statement(s):

I have read and understood the information sheet (12/10/2016) and have had the opportunity to ask questions about the study. □

I agree to take part in this research project and agree for my data to be used for the purpose of this study □

I understand my participation is voluntary and I may withdraw at any time without my legal rights being affected □

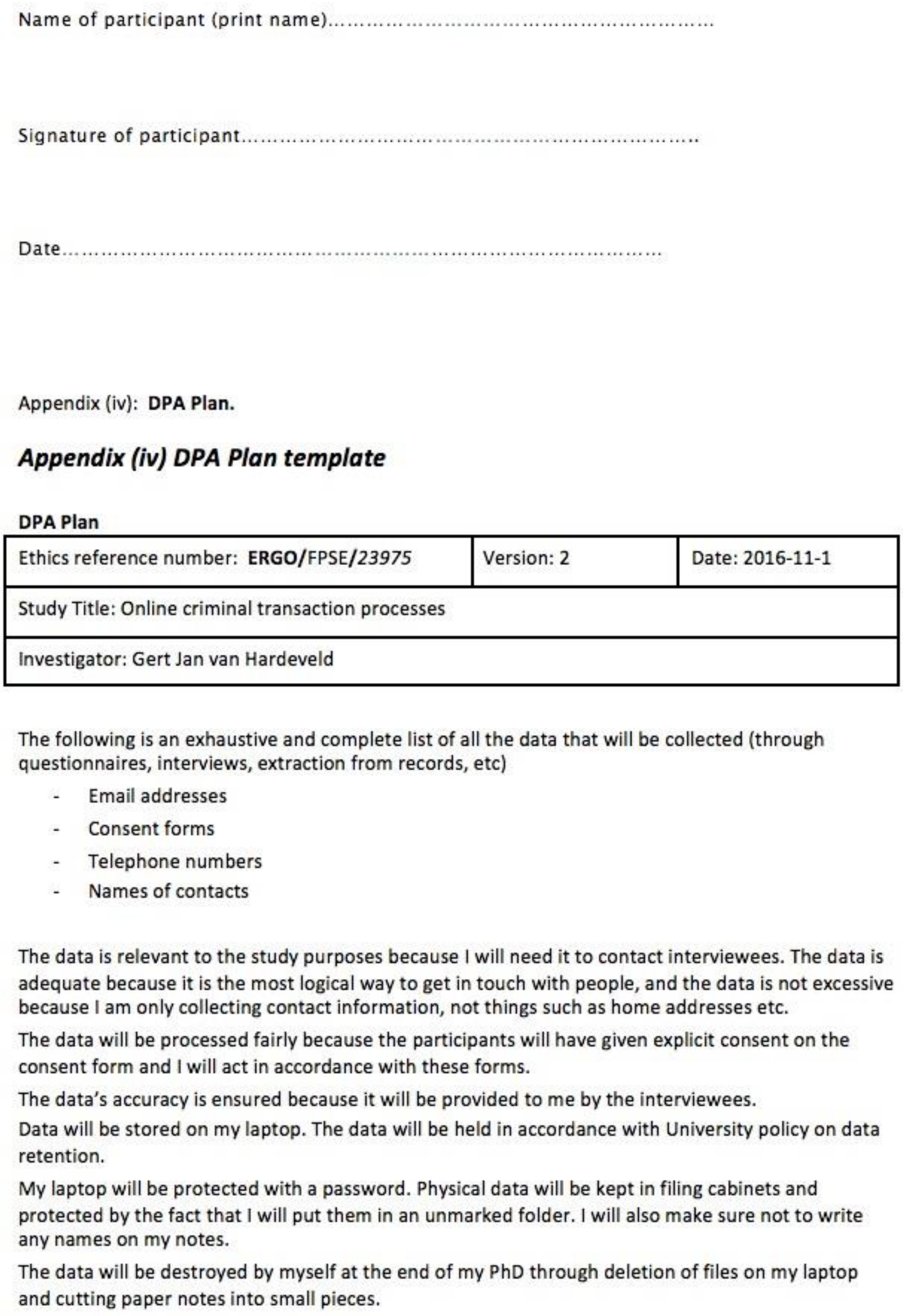
I consent to being interviewed □

I consent to this interview being recorded □

Data Protection

I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.

Appendix E



Name of participant (print name)……………………………………………………

Signature of participant………………………………………………………………

Date……………………………………………………………………………………

Appendix (iv): **DPA Plan.**

Appendix (iv) DPA Plan template

DPA Plan

Ethics reference number: **ERGO/**FPSE**/***23975*	Version: 2	Date: 2016-11-1
Study Title: Online criminal transaction processes		
Investigator: Gert Jan van Hardeveld		

The following is an exhaustive and complete list of all the data that will be collected (through questionnaires, interviews, extraction from records, etc)

- Email addresses
- Consent forms
- Telephone numbers
- Names of contacts

The data is relevant to the study purposes because I will need it to contact interviewees. The data is adequate because it is the most logical way to get in touch with people, and the data is not excessive because I am only collecting contact information, not things such as home addresses etc.

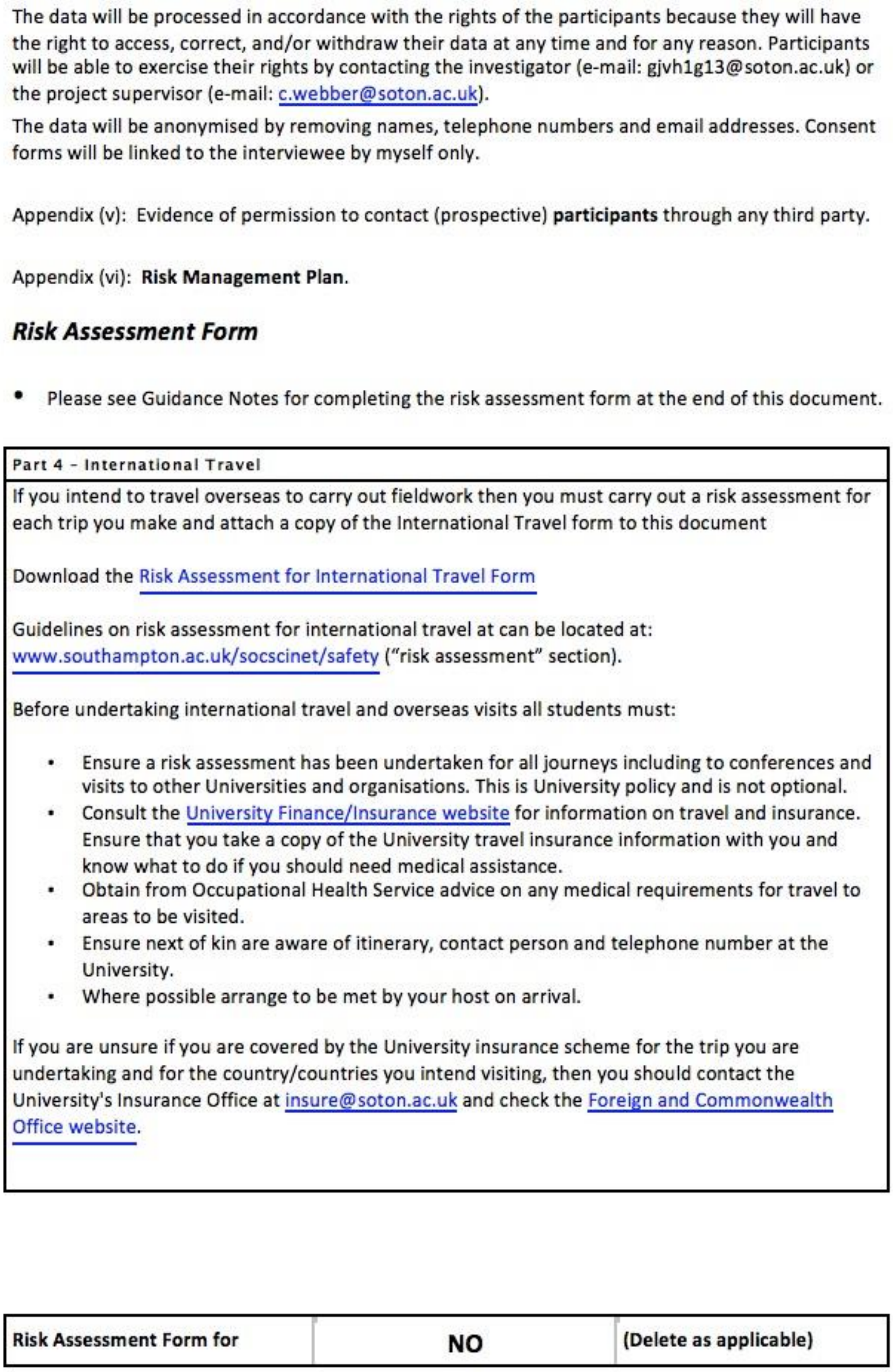
The data will be processed fairly because the participants will have given explicit consent on the consent form and I will act in accordance with these forms.

The data's accuracy is ensured because it will be provided to me by the interviewees.

Data will be stored on my laptop. The data will be held in accordance with University policy on data retention.

My laptop will be protected with a password. Physical data will be kept in filing cabinets and protected by the fact that I will put them in an unmarked folder. I will also make sure not to write any names on my notes.

The data will be destroyed by myself at the end of my PhD through deletion of files on my laptop and cutting paper notes into small pieces.



The data will be processed in accordance with the rights of the participants because they will have the right to access, correct, and/or withdraw their data at any time and for any reason. Participants will be able to exercise their rights by contacting the investigator (e-mail: gjvh1g13@soton.ac.uk) or the project supervisor (e-mail: c.webber@soton.ac.uk).

The data will be anonymised by removing names, telephone numbers and email addresses. Consent forms will be linked to the interviewee by myself only.

Appendix (v): Evidence of permission to contact (prospective) **participants** through any third party.

Appendix (vi): **Risk Management Plan.**

Risk Assessment Form

- Please see Guidance Notes for completing the risk assessment form at the end of this document.

Part 4 - International Travel

If you intend to travel overseas to carry out fieldwork then you must carry out a risk assessment for each trip you make and attach a copy of the International Travel form to this document

Download the Risk Assessment for International Travel Form

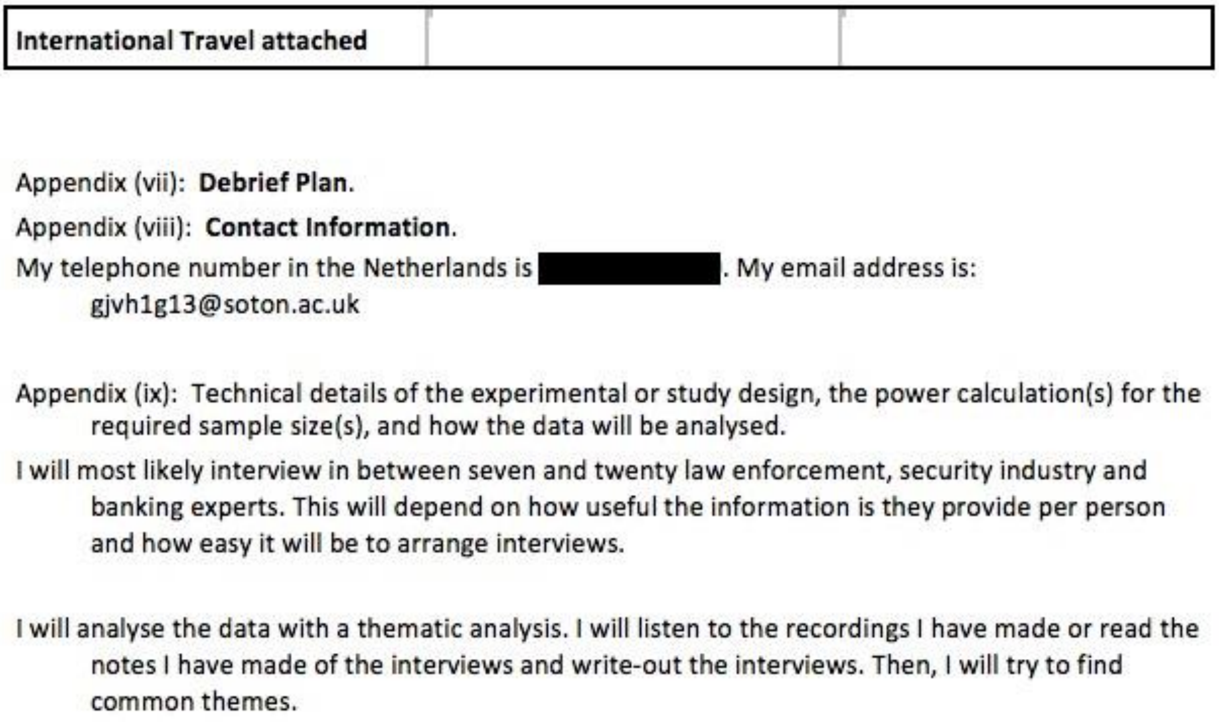
Guidelines on risk assessment for international travel at can be located at: www.southampton.ac.uk/socscinet/safety ("risk assessment" section).

Before undertaking international travel and overseas visits all students must:

- Ensure a risk assessment has been undertaken for all journeys including to conferences and visits to other Universities and organisations. This is University policy and is not optional.
- Consult the University Finance/Insurance website for information on travel and insurance. Ensure that you take a copy of the University travel insurance information with you and know what to do if you should need medical assistance.
- Obtain from Occupational Health Service advice on any medical requirements for travel to areas to be visited.
- Ensure next of kin are aware of itinerary, contact person and telephone number at the University.
- Where possible arrange to be met by your host on arrival.

If you are unsure if you are covered by the University insurance scheme for the trip you are undertaking and for the country/countries you intend visiting, then you should contact the University's Insurance Office at insure@soton.ac.uk and check the Foreign and Commonwealth Office website.

Risk Assessment Form for	**NO**	**(Delete as applicable)**



International Travel attached		

Appendix (vii): **Debrief Plan**.

Appendix (viii): **Contact Information**.

My telephone number in the Netherlands is [redacted]. My email address is: gjvh1g13@soton.ac.uk

Appendix (ix): Technical details of the experimental or study design, the power calculation(s) for the required sample size(s), and how the data will be analysed.

I will most likely interview in between seven and twenty law enforcement, security industry and banking experts. This will depend on how useful the information is they provide per person and how easy it will be to arrange interviews.

I will analyse the data with a thematic analysis. I will listen to the recordings I have made or read the notes I have made of the interviews and write-out the interviews. Then, I will try to find common themes.

List of References

Afilipoaie, A., & Shortis, P. (2015). Operation Onymous: International law enforcement agencies target the Dark Net in November 2014. *Global Drug Policy Observatory*. Retrieved from https://www.swansea.ac.uk/media/GDPO%20SA%20Onymous.pdf.

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). Honor among thieves: A common's analysis of cybercrime economies. *eCrime Researchers Summit*, 1–11.

Afroz, S., Caliskan-Islam, A., Stolerman, A., Greenstadt, R., & McCoy, D. (2014). Doppelgänger Finder: Taking Stylometry To The Underground. *Proceedings of the 35rd Conference on IEEE Symposium on Security and Privacy*, 212–226.

Aldridge, J. & Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. Available at SSRN: https://ssrn.com/abstract=2436643.

Aldridge, J. & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109.

Akerlof, G. A. (1970). The Market For Lemons: Quality Uncertainty and The Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488-500.

Akers, R. L. (1977). *Deviant Behavior: A Social Learning Approach* (Second edition). Belmont, California, USA: Wadsworth Publishing Company, Inc.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social Learning and Deviant Behavior: A Specific Test of a General Theory. *American Sociological Review*, *44*(4), 636–655.

Akers, R. L. (1990). Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. *The Journal of Criminal Law & Criminology*, *81*(5), 653–676.

Allodi, L., Corradin, M., & Massacci, F. (2016). Then and Now: On the Maturity of the Cybercrime Markets. The Lesson That Black-Hat Marketeers Learned. *IEEE Transactions on Emerging Topics in Computing*, *4*(1), 35–46.

Anderson, R., Barton, C., Rainer, B., Clayton, R., Eeten, M. J. G. Van, Levi, M., Moore, T. and Savage, S. (2012). Measuring the Cost of Cybercrime. *Workshop on Economics of Information Security*, 1–31.

Australian Payments Clearing Association. (2014). *Australian Payments Fraud. Details and Data 2014*. Retrieved from http://www.apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2014.pdf.

Australian Payments Clearing Association. (2015). *Australian Payments Fraud. Details and Data 2015*. Retrieved from http://www.apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2015.pdf.

Australian Payments Clearing Association. (2016). *Australian Payments Fraud. Details and Data 2016*. Retrieved from http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf.

Australian Payments Clearing Association. (2017). Australian Payments Fraud 2017. Jan-Dec 2016 Data. Retrieved from http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2017.pdf.

Bada, M., Sasse, A.M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In *Proceedings of the International Conference on Cyber Security for Sustainable Society,* 118–131.

Balogun, A., & Zhu, S. (2013). Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology. *International Journal of Advanced Computer Science and Applications*, *4*(5), 36–40.

Barratt, M. J. (2012). Silk Road: Ebay for Drugs. *Addiction*, *107*(3): 683.

Batarseh, F. (2011). *Incremental Lifecycle Validation of Knowledge-Based Systems Through CommonKADS*. PhD Thesis. University of Central Florida.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *The Journal of Political Economy*, *76*, 169–217.

Becker, G. S. (1976). *The Economics Approach to Human Behavior*. Chicago: The University of Chicago Press.

Berners-Lee, T., Hall, W., Hendler, J., Shadbolt, N. & Weitzner, D. J. (2006a). Creating a Science of the Web. *Science*, *313*(5788), 769–771.

Berners-Lee, T., Hall, W., Hendler, J. A., O'Hara, K., Shadbolt, N. & Weitzner, D. J. (2006b). A Framework for Web Science. *Foundations and Trends in Web Science*, *1*(1), 1–130.

Bernoulli, D. (1738/1954). Exposition of a new theory on the measurement of risk. *Econometrica*, *22*(1), 23–36.

Bidgoli, M., & Grossklags, J. (2017). “Hello. This is the IRS calling.”: A Case Study on Scams, Extortion, Impersonation, and Phone Spoofing. In *Proceedings of the Symposium on Electronic Crime Research*.

Biryukov, A., Pustogarov, I., & Weinmann, R. (2013). Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. In Proceedings of *IEEE Symposium on Security and Privacy*, 80–94.

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 15–29.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *The Journal of Economic Perspectives*, *29*(2), 213-238.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, *2*(6), 1-12.

Bossler, A. M., & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bourdieu, P. (1984). *Distinction. A Social Critique of the Judgement of Taste*. Cambridge: Harvard University Press

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Brayley, H., Cockbain, E., & Laycock, G. (2011). The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking. *Policing*, *5*(2), 132–143.

British Society of Criminology. (2015). British Society of Criminology Statement of Ethics for Researchers. Available at http://www.britsoccrim.org/documents/BSCEthics2015.pdf.

Brito, J., Shadab, H., & Castillo, A. (2014). Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling. *The Columbia Science & Technology Law Review*, 16, 144–221.

Bromby, M., Macmillan, M., & Mckellar, P. (2003). A CommonKADS Representation for a Knowledge-based System to Evaluate Eyewitness Identification. *International Review of Law, Computers & Technology*, *17*(1), 99–108.

Buxton, J., & Bingham, T. (2015). The Rise and Challenge of Dark Net Drug Markets. *Global Drug Policy Observatory*, *policy brief 7*. Available at https://www.swansea.ac.uk/media/The%20Rise%20and%20Challenge%20of%20Dark%20Net%20Drug%20Markets.pdf.

Byrne, B. (2004). Qualitative Interviewing. In C. Seale (Ed.), *Researching Society and Culture* (Second Edition). London: SAGE.

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26–38.

Chiu, Y.N., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories: Implications for Prevention. *British Journal of Criminology*, *51*(2), 355–374.

Chon, S., & Broadhurst, R. (2014). *Routine Activity Theory and Cybercrime: What about Offender Resources?* Working Paper. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379201.

Clarke, R. V. (1983). Situational Crime Prevention: Its Theoretical Basis and Practical Scope. *Crime and Justice*, *4*, 225-256.

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, 19, 91-150.

Clarke, R. V. (1997). *Situational Crime Prevention. Successful Case Studies* (Second edition). Albany, N.Y.: Harrow and Heston.

Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University Law Review*, *40*(3), 698–736.

Cohen, A. K. (1956). *Delinquent Boys. The Culture of the Gang*. London: Routledge & Kegan Paul Ltd.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608.

Cornish, D. (1994). The Procedural Analysis of Offending and its Relevance for Situational Crime Prevention. In Clarke, R.V. (Ed.), *Crime Prevention Studies Volume 3*, 151–196. Monsey, NY: Criminal Justice Press.

Cornish D.B. and Clarke R.V. (1986). *The Reasoning Criminal. Rational choice perspectives on criminal offending*. New York: Springer-Verlag. Cornish

Cornish, D. B., and Clarke, R. V. (2003). Opportunities, Precipitators, and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. *Crime Prevention Studies* 16, 41–96.

Council of Europe. (2001). Convention on Cybercrime. Retrieved from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (2017). *Implementation of Article 13 Budapest Convention by Parties and Observers: Assessment Report*. Retrieved from https://rm.coe.int/t-cy-2015-18-implementation-of-article-13-budapest-convention-by-parti/1680724ca4

Cox, J. (2016). Staying in the shadows: the use of bitcoin and encryption in cryptomarkets. In EMCDDA project group (Eds.), *The internet and drug markets*, 41-47. Publications office of the European Union: Luxembourg.

Cross, C., Richards, K., & Smith, R. (2016). *Improving responses to online fraud victims: An examination of reporting and support*. Canberra: Criminology Research Advisory Council. Retrieved from http://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf.

Cross, C. (2018). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South*, 261–280. Palgrave Macmillan.

Cybercrime Convention Committee. (2014). *T-CY Assessment Report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*. Retrieved from: https://rm.coe.int/16802e726c.

Day, M. J., Carr, L. & Halford, S. (2015). Developing the "Pro-human" Web. In *Proceedings of Web Science 2015*, 1-10.

De Nederlandsche Bank, & Betaalvereniging Nederland. (2017). *Betalen aan de kassa 2016*. Retrieved from https://www.betaalvereniging.nl/wp-uploads/2017/04/Factsheet_Betalen_ad_kassa.pdf.

Décary-Hétu, D., & Leppänen, A. (2013). Criminals and signals: An assessment of criminal performance in the carding underworld. *Security Journal*, *29*(3), 442-460.

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, *14*(2-3), 1-22.

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the Net: Monitoring of Online Offenders by Researchers. *The European Review of Organised Crime*, *2*(2), 122-141.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75.

Décary-Hétu, D. & Lavoie, M. (2018) BitCluster: outil d'analyse des bitcoins, une transaction à la fois. In Décary-Hétu, D. & Bérubé, M. (Eds.). *Délinquance et innovation*. Montréal, Canada: University of Montréal Press.

Demant, J., Aldridge, J., Décary-Hétu, D., & Munksgaard, R. (2018). Going Local on a Global Platform: A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime. *International Criminal Justice Review*, 1–20. Available at http://doi.org/10.1177/1057567718769719.

Dexter, L. A. (1970). *Elite and Specialized Interviewing*. Evanston, Illinois, USA: Northwestern University Press.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium*.

Doeland, M. (2017). Collaboration and the sharing of information help reduce payment transactions fraud. *Journal of Payments Strategy & Systems*, *11*(1), 81–85.

Donnermeyer, J. F., & DeKeseredy, W. (2008). Toward a rural critical criminology. *Southern Rural Sociology*, *23*(2), 4–28.

Dorussen, H., Lenz, H., & Blavourkos, S. (2005). Assessing the Reliability and Validity of Expert Interviews. *European Union Politics*, *6*(3), 315–337.

Douceur, J. R. (2002). The Sybil Attack. In *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 1-6.

Dupont, B., Côté, A.M., Boutin, J.I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." *American Behavioral Scientist*, *61*(11), 1219–1243.

Dutch Banking Association & Dutch Payments Association (2017). Fact Sheet Payments. https://www.nvb.nl/media/document/002088_nvb-fact-sheet-payments.pdf

Dutch Banking Association (2017). Fact Sheet Security and Fraud. https://www.nvb.nl/feiten-cijfers/2094/veiligheid-en-fraude.html

Duxbury, S. W., & Haynie, D. L. (2017). The Network Structure of Opioid Distribution on a Darknet Cryptomarket. *Journal of Quantitative Criminology*, 1-21. Retrieved from https://link.springer.com/article/10.1007/s10940-017-9359-4.

Dykstra, J., & Sherman, A. T. (2011). Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies. *Journal of Network Forensics*, *3*(1), 19–31.

Ekblom, P., & Gill, M. (2016). Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime. *European Journal on Criminal Policy and Research*, *22*(2), 319–339.

European Central Bank (ECB). (2015). *Fourth report on card fraud*. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf.

Europol. (2014). *The Internet Organised Crime Threat Assessment (iOCTA)*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf.

Europol. (2016). The Internet Organised Crime Threat Assessment. Retrieved from https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016.

Europol. (2017). The Internet Organised Crime Threat Assessment. Retrieved from https://www.europol.europa.eu/iocta/2017/index.html.

Eurojust & Europol. (2017). Common challenges in combating cybercrime. Version 2.0. Retrieved from http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf.

European Parliament & European Council. (2015). *Directive on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC*. Retrieved from http://data.consilium.europa.eu/doc/document/PE-35-2015-INIT/en/pdf

European Parliament. (2017). *Report on the proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and amending Directive 2009/101/EC*. Retrieved from: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0056+0+DOC+XML+V0//EN

Eysenbach, G., & Till, J. (2001). Ethical issues in qualitative research on internet communities. *BMJ*, *323*, 1103–1105.

Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information Systems Frontiers*, *15*(1), 5–15.

The Federal Reserve. (2016). *The Federal Reserve Payments Study 2016*. Retrieved from https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief. Practical theory for crime prevention. *Police Research Series*, *Paper 98*.

Ferrell, J. (1997). Criminological verstehen: Inside the immediacy of crime. *Justice Quarterly*, *14*(1), 3-23.

Ferrell, J. (2004). Boredom, Crime and Criminology. *Theoretical Criminology*, *8*(3), 287–302.

Financial Fraud Action UK. (2014). *Fraud The Facts 2014. The definitive overview of payment industry fraud and measures to prevent it*.

Financial Fraud Action UK. (2015). *Fraud the facts 2015. The definitive overview of payment industry fraud and measures to prevent it*.

Financial Fraud Action UK. (2016). *Fraud the facts 2016. The definitive overview of payment industry fraud*.

Financial Fraud Action UK. (2017). *Fraud the facts 2017. The definitive overview of payment industry fraud*.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 375–388.

Garg, V., & Camp, L. J. (2015). Why Cybercrime ? *SIGCAS Computers & Society*, *45*(2), 20–28.

Garland, D. (2001). *The Culture of Control. Crime and Societal Order in Contemporary Society*. Oxford: Oxford University Press.

Garoupa, N. (2003). Behavioral Economic Analysis of Crime: A Critical Review. *European Journal of Law and Economics*, *15*(1), 5–15.

German Federal Office for Information Security. (2015). Security Analysis of TrueCrypt. Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Truecrypt/Truecrypt.pdf?__blob=publicationFile&v=2.

Giddens, A. (1984). *The Constitution of Society. Outline of the theory of structuration*. Cambridge: Polity Press.

Giddens, A. (1996). *The Consequences of Modernity*. Cambridge: Polity Press.

Gilmour, N. (2014). Understanding Money Laundering – A Crime Script Approach. *The European Review of Organised Crime*, *1*(2), 35–56.

Glenny, M. (2011). Darkmarket: Cyberthieves, cybercops and you. London: The Bodley Head.

Göbel, J., Holz, T., & Trinius, P. (2009). Towards Proactive Spam Filtering. In U. Flegel & D. Bruschi (Eds.), *Detection of Intrusions and Malware and Vulnerability Assessment* (pp. 38–47). Como, Italy: Springer.

Goldfeder, S., Bonneau, J., Gennaro, R., & Narayanan, A. (2017). Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin. In *Proceedings of Financial Cryptography and Data Security*, 1–27.

Goldstein, H. (1979). Improving Policing - A Problem Oriented Approach. *Crime & Delinquency*, *25*, 236–258.

Goncharov, M. (2015). Russian Underground 2.0. Cupertina, CA: Trend Micro Incorperated.

Grabosky, P.N. (1996). Uninted Consequences of Crime Prevention. In R. Homel and J. Clarke (eds), *Crime Prevention Studies*, *5*, 25-56.

Guitton, C. (2013). A review of the available content on Tor hidden services: The case against further development. *Computers in Human Behavior*, *29*(6), 2805–2815.

Gül, S. K. (2009). An Evaluation of the Rational Choice Theory in Criminology. *Journal of Social and Applied Sciences*, *4*(8), 36–44.

Gupta, D., Tiwari, G., Kapoor, Y., & Kumar, D. P. (2009). Mac Spoofing and its Countermeasures. *International Journal of Recent Trends in Engineering*, *2*(4), 1–2.

Guthrie, C. (2002). Prospect theory, risk preference, and the law. *Northwestern University Law Review*, *97*(3), 1115–1164.

Halford, S., Pope, C. & Carr, L. (2010). A Manifesto for Web Science? In *Proceedings of the WebSci10: Extending the Frontiers of Society On-Line*, 1–6.

Halford, S. (2017). The Ethical Disruptions of Social Media Data: Tales from the Field. In K. Woodfield (Ed.), *The Ethics of Internet-mediated research and using social media for social research*. Bingley, UK: Emerald Group Publishing.

Hall, W. (2011). The Ever Evolving Web: The Power of Networks. *International Journal of Communication*, *5*, 651–664.

Harrell, E. (2015). Victims of Identity Theft, 2014. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. NCJ 248991, p. 1–26.

Hay, B. & Webster, J. (2014). Responding to organised payment card compromise and subsequent fraud. *Journal of Payments Strategy & Systems*, *8*(1), 30–42.

Hayashi, F., Moore, T., & Sullivan, R. J. (2015). The Economics of Retail Payments Security. In *Fifth International Payments Policy Conference: The Puzzle of Payments Security, Federal Reserve Bank of Kansas City*, 1–60.

Hayward, K. J., & Young, J. (2004). Cultural criminology: Some notes on the script. *Theoretical Criminology*, *8*(3), 259–273.

Hayward, K. J. (2016). Cultural criminology: Script rewrites. *Theoretical Criminology*, *20*(3), 297–321.

Hawkins, S., Yen, D. C., & Chou, D. C. (2000). Awareness and challenges of Internet security. *Information Management & Computer Security*, *8*(3), 131–143.

Healey, N. J., Angelopoulou, O., & Evans, D. (2013). A discussion on the recovery of data from a virtual machine. *Proceedings of the 4th International Conference on Emerging Intelligent Data and Web Technologies*, 603–606.

Hendler, J., Shadbolt, N., Hall, W., Berners-Lee, T., & Weitzner, D. J. (2008). Web Science : An Interdisciplinary Approach to Understanding. *Communications of the ACM*, *51*(7), 60–69.

Hershey, J. C., & Schoemaker, P. J. H. (1980). Risk Taking and Problem Context in the Domain of Losses : An Expected Utility Analysis. *The Journal of Risk and Insurance*, *47*(1), 111–132.

Hesseling, R. (1994). Displacement: A review of the empirical literature. *Crime Prevention Studies*, *3*, 197–230.

Hobson, D. (2013). What is Bitcoin? *XRDS: Crossroads, The ACM Magazine for Students*, *20*(1), 40–44.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25.

Holt, T. J. (2010). Examining the Language of Carders. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime*, 127–143. Hershey, PA: Information Science Reference.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40.

Holt, T. J., Bossler, A. M., Malinski, R. & May, D.C. (2015). Identifying Predictors of Unwanted Sexual Conversations Among Youth Using a Low Self-Control and Routine Activity Theory Framework. *Journal of Contemporary Criminal Justice*, *32*(2), 108-128.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137–145.

Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime*, *18*(1), 1–10.

Horton-Eddison, M. & Di Cristofaro, M. (2017). *Hard Interventions and Innovation in Crypto-Drug Markets : The escrow example*. Retrieved from http://www.swansea.ac.uk/media/Escrow_PB11_GDPO_AUGUST2017.pdf

Horton-Eddison, M. (2017). *Updating Escrow: Demystifying the CDM multisig process*. Global Durg Policy Observatory Situation Analysis. Retrieved from http://www.swansea.ac.uk/media/HortonEddisonGDPOMultiSigEscrowSA.pdf

Hout, M. C. Van, & Bingham, T. (2013). "Silk Road", the virtual drug marketplace: a single case study of user experiences. *The International Journal on Drug Policy*, *24*(5), 385–391.

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior*, *37*(10), 1163–1178.

Hutchings, A., Clayton, R., & Anderson, R. (2016). Taking Down Websites to Prevent Crime. In Proceedings of *eCrime*, 1-10.

Hutchings, A., & Clayton, R. (2017). Configuring Zeus: A case study of online crime target selection and knowledge transmission. In Proceedings of *eCrime*, 1-8.

Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology*, *55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11-30.

Hyman, P. (2013). Cybercrime: It’s Serious, But Exactly how Serious? *Communications of the ACM*, *56*(3), 18–20.

Ianelli, N., & Hackworth, A. (2007). Botnets as a Vehicle for Online Crime. *The International Journal of Forensic Computer Science*, *1*, 19–39.

INTERPOL (2016). Fact Sheet. Capacity Building and Training. https://www.interpol.int/content/download/19244/170106/version/20/file/07_GI07_02_2016_EN_web.pdf

INTERPOL (2017). Illegal Wildlife Trade in the Darknet. Retrieved from https://www.interpol.int/News-and-media/News/2017/N2017-080.

Israel, M. (2004). Strictly Confidential? Integrity and the Disclosure of Criminological and Socio-Legal Research. *British Journal of Criminology*, *44*(5), 715-740.

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing, (21). Global Commission on Internet Governance paper series no. 21. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.

Jervis, R. (2004). The Implications of Prospect Theory for Human Nature and Values. *Political Psychology*, *25*(2), 163-176.

Jolls, C., Sunstein, C. R., & Thaler, R. (1998). A Behavioral Approach to Law and Economics. *Stanford Law Review*, *50*, 1471-1550.

Juran, J. (1954). Universals in Management Planning and Controlling. *The Management Review*, *43*(11), 748-761.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-292.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives*, *5*(1), 193-206.

Kahneman, D., & Frederick, S. (2002). Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics of Intuitive Judgment: Extensions and Applications*, 49-81. New York: Cambridge University Press.

Kahneman, D. (2003). A Perspective on Judgment and Choice. Mapping Bounded Rationality. *American Psychologist*, *58*(9), 697–720.

Kahneman, D. (2011). *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kaspersky Lab. (2016a). The xDdedic Marketplace. Retrieved from https://securelist.com/files/2016/06/xDedic_marketplace_ENG.pdf.

Kaspersky Lab. (2016b). The Tip of the Iceberg. An Unexpected Turn in the xDedic story. Retrieved from https://securelist.com/blog/research/75120/the-tip-of-the-iceberg-an-unexpected-turn-in-the-xdedic-story/.

Kaspersky Lab & INTERPOL. (2017). Mobile Malware Evolution 2016. Retrieved from https://securelist.com/files/2017/02/Mobile_report_2016.pdf.

Kigerl, A. (2011). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, *30*(4), 470-486.

Kirlappos, I., Beautement, A., & Sasse, M. A. (2013). “Comply or Die” Is Dead: Long live security-aware principal agents. In *Proceedings of Workshop on Usable Security*. Okinawa, Japan.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from “Shadow Security:” Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. In *Proceedings of Workshop on Usable Security*. San Diego, USA.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands*. RAND, Europe: Cambridge, UK. Available at http://www.rand.org/pubs/research_reports/RR1607.html.

Ladegaard, I. (2017). We Know Where You Are, What You Are Doing and We Will Catch You. Testing Deterrence Theory in Digital Drug Markets. *British Journal of Criminology*, 1–20. Retrieved from https://doi.org/10.1093/bjc/azx021.

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature, *Crime Science*, *3*(9), 1–10.

Lattimore, P., & Witte, A. (1986). Models of Decision Making Under Uncertainty: The Criminal Choice. In R. V Clarke & D. Cornish (Eds.), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, 129-155. New Brunswick, New Jersey: Springer-Verlag.

Lavorgna, A. (2013). Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes. PhD Thesis. University of Trento.

Lavorgna, A. (2014). Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics. *Trends in Organized Crime*, *17*(4), 250–270.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals : New criminal opportunities , trends and challenges. *European Journal of Criminology*, *12*(2), 226–241.

Lea, J. (2015). Jock Young and the Development of Left Realist Criminology. *Critical Criminology*, *23*(2), 165–177.

Lea, J. (2016). Left Realism: A Radical Criminology for the Current Crisis. *International Journal for Crime, Justice and Social Democracy*, *5*(3), 53-65.

Leontiadis, N. (2014). *Structuring disincentives for online criminals*. PhD Thesis. Carnegie Mellon University.

Leontiadis, N., & Hutchings, A. (2015). Scripting the crime commission process in the illicit online prescription drug trade. *Journal of Cybersecurity*, *1*(1), 81–92.

Leukfeldt, E. R. (2014a). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

Leukfeldt, E. R. (2014b). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime*, *17*(June), 231–249.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime : A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280.

Leukfeldt, R., Lavorgna, A., & Kleemans, E. R. (2016). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300.

Leukfeldt, R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology, 57*(3), 704-722.

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist*, *61*(11), 1387–1402.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice*, *8*(4), 389–419.

Lewman, A. (2016). Tor and links with cryptomarkets. In EMCDDA project group (Eds.), *The internet and drug markets*, 33-39. Publications office of the European Union: Luxembourg.

Li, B., Erdin, E., Gunes, M. H., Bebis, G., & Shipley, T. (2013). An overview of anonymity technology usage. *Computer Communications*, *36*(12), 1269–1283.

Lord, N., Benson, K., Bellotti, E., & Benson, K. (2017). A script analysis of the distribution of counterfeit alcohol across two European jurisdictions. *Trends in Organized Crime*, *20*(3-4), 252–272.

Loveday, B. (2017). Still Plodding Along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science & Management*, *19*(2), 101–109.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, *13*(2), 71–94.

Lusthaus, J. & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice*, 1–11. Retrieved from http://doi.org/10.1093/police/pax042.

Maimon, D., Kamerdze, A., Cukier, M. & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the Routine Activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343.

Marcum, C.D., Higgins, G.E. & Ricketts, M.E. (2010). Potential Factors of Online Victimization of Youth: An Examanition of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, *31*(5), 381-410.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the "cryptomarket." *Criminology and Criminal Justice*, *14*(3), 351–367.

Martin, J., & Christin, N. (2016). Ethics in Cryptomarket Research. *International Journal of Drug Policy*, *35*, 84–91.

Matthews, R. (2009). Beyond "so what?" criminology. *Theoretical Criminology*, *13*(3), 341–362.

Matthews, R. (2014). Cultural realism? *Crime, Media, Culture: An International Journal*, *10*(3), 203–214.

McLaughlin, E. (2007). *The New Policing*. London: SAGE Publications Ltd.

McLaughlin, E. (2014). See also Young, 1971: Marshall McLuhan, moral panics and moral indignation. *Theoretical Criminology*, *18*(4), 422–431.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of Bitcoins: Characterizing payments among men with no names. In *Proceedings of the Internet Measurement Conference*, 127–140.

Merton, R. K. (1938). Social Structure and Anomie. *American Sociological Review*, *3*(5), 672–682.

Michnowicz, R.G. (2006). OPSEC In The Information Age. USAWC Strategy Research Project. Carlisle, PA: U.S. Army War College, 1-16. Retrieved from: http://ssi.armywarcollege.edu/pdffiles/ksil427.pdf.

Minch, R.P. (2015). Location Privacy in the Era of the Internet of Things and Big Data Analytics. In *proceedings of the 48th Hawaii International Conference on System Sciences*, 1521-1530.

Møller, K., Munksgaard, R., & Demant, J. (2017). "Flow My FE the Vendor Said": Conceptualizing Thefts and Frauds on Cryptomarkets for Illicit Drugs. *American Behavioral Scientist*, *61*(11), 1427–1450.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economies of Online Crime. *Journal of Economic Perspectives*, *23*(3), 3–20.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, *7859*, 25–33.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival. Global Politics and Strategy*, *58*(1), 7–38.

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review*, *27*(4), 237-254.

Moser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In *Proceedings of IEEE eCrime Researchers Summit*.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An Analysis Of Underground Forums. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement*, 71-79.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf.

Nãsi, M., Oksanen, A., Keipi, T. & Rãsãnen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210.

National Crime Agency (NCA). (2016). *Cyber Crime Assessment 2016*. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

National Crime Agency (NCA). (2017). *Pathways Into Cyber Crime*. Retrieved from: http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file

Ngo, F.T. & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

O'Hara, K. (2004). *Trust: From Socrates to Spin*. Cambridge, UK: Icon Books.

O'Hara, K. (2012). Trust from the Enlightenment to the Digital Enlightenment. In Bus, J., Crompton, M., Hildebrandt, M. & Metakides, G. (Ed.), *Digital Enlightenment Yearbook 2012*, 169–183. IOS Press.

Omand, D. (2015). The Dark Net: Policing the Internet's Underworld. *World Policy Journal*, (Winter 2015/2016). Retrieved from http://www.worldpolicy.org/journal/winter2015/dark-net.

Ogden, J., Halford, S., & Carr, L. (2017). Observing Web Archives. The Case for an Ethnographic Study of Web Archiving. In *Proceedings of Web Science 2017*, 1-10.

Ouytsel, J. van, Ponnet, K. & Walrave, M. (2016). Cyber Dating Abuse Victimization Among Secondary School Students From a Lifestyle-Routine Activities Theory Perspective. *Journal of Interpersonal Violence*, *33*(17), 2767-2776.

Øverlier, L., & Syverson, P. (2006). Locating Hidden Services. *In Proceedings of the IEEE Symposium on Security and Privacy*, 100–114.

Pandey, A., & Saini, J. R. (2012). Counter Measures to Combat Misuses of MAC Address Spoofing Techniques. *International Journal of Advanced Networking and Applications*, *3*(5), 1358–1361.

Patton, M. (1990). Purposeful Sampling. *Qualitative Evaluation and Research Methods*, 169–186.

Paulissen, L., & Wilsem, J. van. (2015). Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland. *Politiewetenschap*, *82*, 1-106.

The Paypers (2016). Ecommerce Payment Methods Report 2016 – Global Payments Insights. Retrieved from https://www.thepaypers.com/reports/ecommerce-payment-methods-report-2016-global-payments-insights/r765256

Peretti, K. (2009). Data Breaches : What the Underground World of Carding Reveals. *Santa Clara High Technology Law Journal*, *25*(2), 375–413.

Pinch T. J. & Bijker W. E. (1989). The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. In Bijker W. E., Hughes T. P. and Pinch T. J. (*Eds.) The Social Construction of Technological Systems: New Directions in the Sociology and History of* Technology, 17-50. Cambridge, MA, USA: MIT Press.

Post, W., Wielinga, B., Hoog, R. De, & Schreiber, G. (1997). Organizational Modeling in CommonKADS: The Emergency Medical Service. *IEEE Expert*, *12*(4), 46–52.

Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, *16*(4), 482–494.

Reid, F., & Harrigan, M. (2013). An Analysis of Anonymity in the Bitcoin System. In Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, & A. Pentland (Eds.), *Security and Privacy in Social Networks*, 197–223. New York, USA: Springer.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Reyns, B.W. & Henson, B. (2015). The Thief With a Thousand Faces and the Victim With None. Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139.

Reyns, B.W., Henson, B. & B.S. Fisher (2015). Guardians of the Cyber Galaxy. An Empirical and Theoretical Analysis of the Guardianship Concept From Routine Activity Theory as it Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 148-168.

Roberts, H., Zucherman, E., York, J., Faris, R., & Palfrey, J. (2010). *2010 Circumvention Tool Usage Report*. Retrieved from https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.

Runciman, W. G. (1966). *Relative deprivation and social justice. A study of attitudes to social inequality in twentieth-century England*. London: Routledge & Kegan Paul Ltd.

Samuelson, W., & Zeckhauser, R. (1988). Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty*, 7–59.

Sawaya, Y., Sharif, M., Christin, N., & Kubota, A. (2017). Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of Conference on Human Factors in Computing Systems,* 2202–2214.

Schank, R., & Abelson, R. (1977). *Scripts Plans Goals and Understanding*. New Jersey: Lawrence Erlbaum Associates.

Schreiber, G., Akkermans, H., Anjewierden, A., Hoog, R. De, Shadbolt, N., Velde, W. Van De, & Wielinga, B. (2000). *The CommonKADS method*. London: The MIT Press.

Seale, C. (2004). Coding and analysing data. In C. Seale (Ed.), *Researching Society and Culture* (Second Edition). London: SAGE.

Shadbolt, N. R., & Smart, P. R. (2015). Knowledge Elicitation: Methods, Tools and Techniques. In J. R. Wilson & S. Sharples (Eds.), *Evaluation of Human Work* (4th edition), 1-43. Boca Raton, Florida, USA: CRC Press.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L., & Hong, J. (2009). Improving Phishing Countermeasures: An Analysis of Expert Interviews. In *Proceedings of the 4th APWG eCrime Researchers Summit*, 1-15.

Smart, P. R., Shadbolt, N. R., & Carr, L. A. & schraefel, m.c. (2005). Knowledge-Based Information Fusion for Improved Situational Awareness. In *Proceedings of 8th International Conference on Information Fusion*, 1017–1024.

Smirnova, O., & Holt, T. J. (2017). Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. *American Behavioral Scientist*, *61*(11), 1403–1426.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In *Proceedings of the 24th USENIX Security Symposium*, 33–48.

Soudijn, M. R. J., & Zegers, B. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*, 111–129.

South Africa Banking Risk Information Centre (SABRIC). (2014). *Card fraud 2013. Protect your card and information at all times*. Retrieved from https://www.sabric.co.za/media/1230/2013-card-fraud-sa-booklet.pdf.

South Africa Banking Risk Information Centre (SABRIC). (2015). *Card fraud 2014. Protect your card and information at all times*. Retrieved from https://www.sabric.co.za/media/1141/final-card-booklet.pdf.

South Africa Banking Risk Information Centre (SABRIC). (2016). *Card fraud 2015. Protect your card and information at all times*. Retrieved from https://www.sabric.co.za/media/1146/final-card-booklet.pdf.

South Africa Banking Risk Information Centre (SABRIC). (2017). *Card Fraud 2016. Protect your card and information at all times. https://www.sabric.co.za/media/1283/2016-card-fraud-booklet.pdf.*

Spagnuolo, M., Maggi, F., & Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. In *Proceedings of the 17th Conference on Financial Cryptography and Data Security*, 457–468.

Spitters, M., Verbruggen, S., & Staalduinen, M. van. (2014). Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden

Services. In *Proceedings of IEEE Joint Intelligence and Security Informatics Conference*, 220–223.

Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: Implications for the rationality debate? *Behavioural and Brain Sciences*, *23*, 645–726.

Studer, R., Benjamins, V. R. & Fensel, D. (1998). Knowledge Engineering: Principles and Methods. *Data & Knowledge Engineering*, *25*(1–2), 161–198.

Sundaresan, S., McCoy, D., Afroz, S., & Paxson, V. (2016). Profiling Underground Merchants Based on Network Behavior. In *Proceedings of the eleventh Symposium on Electronic Crime Research*.

Sunstein, C. R. (1998). Selective Fatalism Social Norms, Social Meaning, and the Economic Analysis of Law. *Journal of Legal Studies*, *27*, 799–824.

Sutton, D., & Patkar, V. (2009). CommonKADS analysis and description of a knowledge based system for the assessment of breast cancer. *Expert Systems with Applications*, *36*(2), 2411–2423.

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664–670.

Tewksbury, R. (2009). Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior for Criminology and Criminal Justice. *Journal of Theoretical and Philosophical Criminology*, *1*(1), 38–58.

Thaler, R. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior and Organization*, *1*(1), 39–60.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge. Improving Decisions About Health, Wealth and Happiness*. New Haven & London: Yale University Press.

Tierney, J. (2010). *Criminology: Theory and context.* Third edition. New York: Prentice Hall.

Tinati, R., Carr, L., Halford, S., & Pope, C. (2013). The HTP Model: Understanding the Development of Social Machines. In Proceedings of *SOCM Workshop, WWW2013: 22nd International World Wide Web conference*, 1-5.

Tinati, R., Carr, L., Halford, S., & Pope, C. (2014). (Re)Integrating the Web: Beyond 'Socio-Technical'. In *Proceedings of the World Wide Web Conference*, 13-17.

Thomas, R., & Martin, J. (2006). the underground economy: priceless. *The USENIX Magazine*, *31*(6), 7–16.

Thomas, K., Yuxing, D., Huang, D., Holt, T. J., Kruegel, C., Mccoy, D., Bursztein, E.,Grier, C., Savage, S. & Vigna, G. (2015). Framing Dependencies Introduced by Underground Commoditization. In *Proceedings of the Workshop on the Economics of Information Security*, 1–24.

Tompson, L., & Chainey, S. (2011). Profiling Illegal Waste Activity: Using Crime Scripts as a Data Collection and Analytical Strategy. *European Journal on Criminal Policy and Research*, *17*, 179–201.

Trend Micro. (2016). *The Cybercriminal Roots of Selling Online Gaming Currency*. Retrieved from http://documents.trendmicro.com/assets/wp/wp-cybercrime-online-gaming-currency.pdf.

Tversky, A., & Kahneman, D. (1986). Rational Choice and the Framing of Decisions. *The Journal of Business*, *59*(4), 251–278.

United Kingdom Government Office for Science. (2016). Distributed Ledger Technology: beyond block chain. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

United States of America v. Alexandre Cazes. (2017). Verified Complaint for Forfeiture *in REM*. Retrieved from https://www.justice.gov/opa/press-release/file/982821/download.

United States of America v. Blake Benthall (2014). Sealed complaint. Retrieved from https://www.scribd.com/document/245744857/Blake-Benthall-Criminal-Complaint.

United States of America v. BTC-E A/K/A Canton Business Corporation and Alexander Vinnik. (2017). Sealed by court order. Retrieved from https://www.justice.gov/usao-ndca/press-release/file/984661/download.

United States of America vs. Liberty Reserve S.A. (2013) Sealed indictment. Retrieved from https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Redacted_0.pdf.

United States of America v. Ross William Ulbricht. (2013). Sealed complaint. Retrieved from https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.

Ulen, T. S. (2000). Rational Choice Theory in Law and Economics. In B. Bouckaert & G. de Geest (Eds.), *Encyclopedia of Law and Economics* (p. 790–818). Cheltenham, UK: Edward Elger.

United Nations Office on Drugs and Crime UNODC. (2016). *World Drug Report*. Retrieved from: https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2015). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169–188.

Vidal, S., & Décary-Hétu, D. (2018). Shake and Bake: Exploring Drug Producers' Adaptability to Legal Restrictions Through Online Methamphetamine Recipes. *Journal of Drug Issues*, *48*(2), 269–284.

Wall, D. S. (2001). *Crime and the Internet*. London: Routledge, Taylor & Francis.

Wall, D.S. (2005). The Internet as a Conduit for Criminal Activity. In A. Pattavina (Ed.), *Information Technology and The Criminal Justice System*, 77–98. Thousand Oaks, California, USA: SAGE Publications Ltd.

Walters, R. (2003). New Modes of Governance and the Commodification of Criminological Knowledge. *Social & Legal Studies*, *12*(1), 5–26.

Warren, S., Oxburgh, G., Briggs, P. & Wall, D. (2017). How might Crime-Scripts be used to Support the Understanding and Policing of Cloud Crime? *Human Aspects of Information Security, Privacy and Trust. Lecture Notes in Computer Science*, *10292*, 539–556.

Webber, C. (2007a). Background, foreground, foresight: The third dimension of cultural criminology? *Crime, Media, Culture*, *3*(2), 139–157.

Webber, C. (2007b). Revaluating relative deprivation theory. *Theoretical Criminology*, *11*(1), 97–120.

Webber, C. (2010). *Psychology & Crime*. London: SAGE Publications Ltd.

Webber, C., & Yip, M. (2013). Drifting on and off-line: humanising the cyber criminal. In S. Winslow & R. Atkinson (Eds.), *New Directions in Crime and Deviancy*. Abington: Routledge, 191–205.

Weber, M. (1987). Economy and Society. An Outline of Interpretative Sociology. Berkeley: University of California Press.

Wegberg, R. van, Verburgh, T., Berg, J. van den, & Staalduinen, M. van. (2017). *Alphabay Exit, Hansa-Down: Dream On? Examining the Effects of Operation Bayonet on Dream Market*. Retrieved from https://www.tno.nl/media/10032/17-9099-factsheetbrochure-dws-05.pdf.

White, S. and White, S. (2016). A research agenda for exploring MOOCs and change in higher education using Socio-Technical Interaction Networks. In *Proceedings of eMOOCs European MOOCs Stakeholder Summit,* 123-134.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology*, *56*(1), 21–48.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, *16*(4), 304–324.

Willison, R., & Lowry, P. (2018). Disentangling the Motivations for Organizational Insider Computer Abuse through the Rational Choice and Life Course Perspectives. *DATABASE for Advances in Information Systems*, *49*(April), 81–102.

Winlow, S., & Hall, S. (2016). Realist Criminology and its Discontents. *International Journal for Crime, Justice and Social Democracy*, *5*(3), 80.

Wortley, R. (2001). A classification of techniques for controlling situational precipitations of crime. *Security Journal*, *14*(4), 63–82.

Yar, M. (2005). The Novelty of “Cybercrime”: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society: An International Journal of Research and Policy*, *23*(4), 1–39.

Yip, M., Shadbolt, N., & Webber, C. (2013). Why forums? An empirical analysis into the facilitating factors of carding forums. In *Proceedings of the 5th Annual ACM Web Science*, 453–462.

Yip, M. (2016). *Cybercrime-as-a-service: An Analysis Into the Facilitating Factors & Social Dynamics of Underground Forums*. PhD thesis. University of Southampton.

Young, J. (1987). The tasks facing a realist criminology. *Contemporary Crises*, *11*(4), 337–356.

Young, J. (1997). Left Realist Criminology: Radical in its Analysis, Realist in its Policy. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The Oxford Handbook of Criminology* (Second edition), 478-491. Oxford: Clarendon Press.

Young, J. (2004). Voodoo Criminology and the Numbers Game. In J. Ferrell, K. J. Hayward, W. Morrison, & M. Presdee (Eds.), *Cultural Criminology Unleashed*, 13-27. London: GlassHouse Press.

Young, J. (2009). Moral Panic. Its Origins in Resistance, Ressentiment and the Translation of Fantasy into Reality. *British Journal of Criminology*, *49*(1), 4–16.

Zawoad, S., & Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Retrieved from http://arxiv.org/abs/1302.6312.