Author:
Van De Sandt, Erik

Title:
Deviant Security

Deviant Security: The Technical Computer Security Practices of Cyber Criminals.

Erik H.A. van de Sandt

26th April 2019

Acknowledgments

What an exciting journey it has been to research deviant security practices while chasing some of the world's most serious and organized cyber criminals. First of all, I thank my amazing supervisor Professor Awais Rashid. You are the perfect example of what impact a cheerful attitude towards life can have on other people. Thank you for your advice, inspiration and support. To all my national and international law-enforcement colleagues with whom I worked during this project, I salute you. The true diversity in backgrounds, cultures and ideas, yet feeling as one big family on a mission, is a bless to me. I could not have done this without you. I love the remark of one of my colleagues who read a first version, and said: 'You basically wrote down what we do, see and discuss on a daily basis'. That is indeed true, and I hope my thesis shows to readers how intellectually satisfying our work is while serving the values of secular liberal democracy. Gert R., Marijn S., Pim T. and Wilbert P., thank you for facilitating me at work. Because of my family and especially my partner S., this felt like fun. Only once, I was insecure about the project, but with your love and support we managed to get me back on track within a week. Thank you.

Abstract

The dominant academic and practitioners' perspective on security evolves around law-abiding referent objects of security who are under attack by law-breaking threat agents. This study turns the current perspective around and presents a new security paradigm. Suspects of crime have threat agents as well, and are therefore in need of security. The study takes cyber criminals as referent objects of security, and researches their technical computer security practices. While their protective practices are not necessarily deemed criminal by law, security policies and mechanisms of cyber criminals frequently deviate from prescribed bonafide cyber security standards. As such, this study is the first to present a full picture on these deviant security practices, based on unique access to public and confidential secondary data related to some of the world's most serious and organized cyber criminals. Besides describing the protection of crime and the criminal, the observed practices are explained by the economics of deviant security: a combination of technical computer security principles and microeconomic theory. The new security paradigm lets us realize that cyber criminals have many countermeasures at their disposal in the preparation, pre-activity, activity and post-activity phases of their *modi operandi*. Their controls are not only driven by technical innovations, but also by cultural, economical, legal and political dimensions on a micro, meso and macro level. Deviant security is very much democratized, and indeed one of the prime causes of today's efficiency and effectiveness crisis in police investigations. Yet every modus operandi comes with all kinds of minor, major and even unavoidable weaknesses, and therefore suggestions are made how police investigations can exploit these vulnerabilities and promote human security as a public good for all citizens. Ultimately, the findings of this socio-technical-legal project prove that deviant security is an academic field of study on its own with continually evolving research opportunities.

Contents

List of Figures

List of Tables

Nomenclature

ACM	Authority for Consumers and Markets
AF	Anti-forensics
AML	Anti-money laundering
APT	Advanced persistent threat
ATM	Automated teller machine
BES	Business enterprise servers
BKA	Bundeskriminalamt
BPH	bulletproof hoster
CC	Command-and-control server
CA	Certificate authority
CaaS	Cyber-crime-as-a-service
CAV	Counter antivirus services
CBA	Cost-benefit analyses
CCS	Cyber crime science
ccTLD	Country code top-level domain
CCTV	Closed-circuit television
CERT	Computer emergency response team
CIA	Confidentiality, integrity and availability
CIS	Commonwealth of Independent States
CPTED	Crime prevention through environmental design
CRI-HR	Cyber criminal community in high-risk areas

CRI-LR	Cyber criminal community in low-risk areas
CS	Computer science
CSAM	Child sexual abuse material
DCCP	Dutch Code of Criminal Procedure
DDoS	Distributed denial-of-service
DevSec	Deviant security
DNA	Deoxyribonucleic acid
DPA	Dutch Police Act
DPC	Dutch Penal Code
EC3	European Cyber Crime Centre of Europol
ECHR	European Convention on Human Rights
ECTF	Electronic Crimes Task Force
ELS	Empirical legal scholarship
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EPO	Electronic purchase order
EU	European Union
FBI	Federal Bureau of Investigation
GDP	Gross domestic product
GPS	Global positioning system
GT	Grounded Theory
IC	Intercultural communication
IC4	International Cyber Crime Coordination Cell
ICD	Incentive centered designs
ID	Identity document
IGCI	Global Complex for Innovation of INTERPOL
IMEI	International mobile equipment identity
IMSI	International mobile subscriber identity
IoC	Indicator of compromise

IP	Internet protocol
ISAC	Information Sharing and Analysis Center
ISP	Internet service provider
IT	Information technology
JCAT	European Joint Cybercrime Action Taskforce
JIT	Joint investigation team
KYC	Know-your-customer
L2TP	Layer 2 Tunneling Protocol
LEA	Law-enforcement agency
LKA	Landeskriminalamt
MAC	Media access control
MBR	Master boot record
MLAT	Mutual legal assistance treaty
MO	Method of operation
MoU	Memoranda of understanding
NCA	National Crime Agency
NCFTA	National Cyber-Forensics Training Alliance
NCI	National critical infrastructure
NCSC	National Cyber Security Center
nEPO	Non-electronic purchase order
NGO	Non-governmental organization
NHTCU	National High Tech Crime Unit
NTD	Notice-and-takedown
OTR	Off-the-Record Messaging
P2p	Peer-to-peer
PET	Privacy-enhancing technology
PKI	Public key infrastructure
PM	Private message system

PPI	Pay-per-install
RAM	Random-access memory
RCP	Rational choice perspective
RDP	Remote desktop protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SBU	Security Service of Ukraine
SEC-HR	Cyber security community in high-risk areas
SEC-LR	Cyber security community in low-risk areas
SMS	Short message system
SOCKS	Socket Secure protocol
SQL	Structured language language
SSL	Secure sockets layer
SWAT	Special weapons and tactics unit
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTP	Tactics, techniques and procedures
US	United States
USSS	United States Secret Service
VM	Virtual machine
VPN	Virtual private network

Chapter 1

Introduction

In February 2015, the daily newspaper The New York Times reported how an automated teller machine (ATM) in Kiev, Ukraine, had started dispensing cash two years earlier whilst no one had even put in a card or touched a button [1]. When a private security firm was called to investigate the case, it discovered that the cause was not a failure or mistake, but an intentional act of crime. The obvious thought was that malicious software was planted on the operating system of the dispensing machine. The security researchers were shocked when they found out that criminals gained unauthorized access to the bank's internal computing systems. Moreover, the attack was not an isolated incident. Over a 100 banks in 30 countries were hacked as well. Besides a malware dubbed Carbanak, the organized crime group installed off-the-shelf remote access tools to learn every move of the bank employees. Therefore, cash outs did not only occur via ATMs, but also through the financial message network of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and personal banking accounts. In short, the criminals monetized whatever internal computer accounts and systems they could get their hands on. By the time of publication, private and public agencies in various countries were alarmed as well, and national computer emergency response teams (CERTs), law-enforcement, the private security industry and the financial sector were working hard to mitigate the threat, prevent further damage, and identify new victims and the perpetrators. What really scared both private and public researchers was that the criminals managed to gain access to the database with the internal financial balance sheets of some banks. Fortunately, the individuals behind the attacks did not harm the availability, confidentiality or integrity of these statements as the consequences to today's globally networked financial system would have been incalculable.

Like similar successful breaches on protective controls of financial institutions, we generally understand this case as an attack by malicious actors on the computing systems of law-abiding entities. From this security perspective, the 'good guys' are the banks that received help from a consortium of private and public agencies, read: the cyber security community. They protect themselves against attacks from constructed ‘bad guys’, i.e., suspects of crime that belong to the cyber criminal community. The law-abiding entities are portrayed as (potential) victims who are predominantly on the defensive side, while the bad guys are seen as malicious attackers who are on the offensive side. The entities that are threatened and therefore the recipients of security - states, businesses and citizens - own legitimate assets safeguarded according to industry standards and/or civil law. The constructed bad guys follow the opposite direction. They are defined as threat agents because of their intentional trespassing of substantive laws, while their attacks do not comply with any law or industry standard. A consequence of this current dominant discourse is that considerable academic, corporate, and governmental efforts are made to improve the security of (potential) victims of cyber crime who are under threat of attacks carried out by cyber criminals (see, for example, [2][3]). In short, the current security discourse evolves around *law-abiding* referent objects who are threatened in their security by threat agents with bad intentions. So the referent object determines our subsequent view on security including who we regard as threat agents [4, p.1163][5, pp.7, 17].

There is, however, a so far less addressed side of this story. The group members behind Carbanak continued to make victims in various corporate sectors until at least late 2017 [6], while a first but important arrest of one of the main coders was only made in April 2018 [7]. Yet the criminal profits remain missing while other groups are successfully using modifications of the Carbanak malware [8]. How is it possible that such a sought after criminal organization was active and its crimes went unpunished for such a long time? For one, criminal investigations are facing heavy weather as too few crimes are currently solved. The Dutch national police even speaks of an effectiveness crisis which affects the legitimacy of the police [9][10][11]. It names the complexity of today’s society as one of the underlying causes, most notably how information technologies create new opportunities to commit crime [12, pp.15-20]. However, would it be possible that information technologies not only promote the commission of crime, but also the protection of crime? In other words, might the security of the bad guys also be one of the causes of the effectiveness crisis in criminal investigations? The answer to this largely rhetorical question is indeed: yes, cyber criminals too can be very much referent objects of security, and this subsequently poses a continuous challenge to legitimate law-enforcement efforts, now and in the future [13, p.6]. Encryption usage for criminal purposes is, for example, central in the ‘going dark’ debate that currently takes place in the United States (US). Former Federal Bureau of Investigation director James B. Comey explained in 2014 how:

> ‘Those charged with protecting our people aren’t always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so’ [14].

In other words, technologies of a protective nature like encryption are used by cyber criminals, rendering technical investigative powers as lawful intercept, preservation and seizure of both data in motion and data at rest useless [15, p.5][16]. As a result, these technologies cause problems for the core investigative process of attribution: determining, and subsequently linking responsibility of a certain *who* to a particular *what* of attacks [17][18][19]. The problems related to *who* refer to the protection of the suspect's identity, and law-enforcement's efforts to determine who is behind an attack (also named the identity problem [20]). The *what* problems refer to protective measures that hinder obtaining evidence relevant to the suspect's criminal activities and thus to determine what kind of attack was carried out [20, p.206][21]. Legal scholar Ian Walden even suggests that the focus in prosecutions will shift to corroborating evidence because cyber criminals will place primary evidence permanently beyond reach of investigators [20, p.393]. If this prediction is true, security practices of cyber criminals not only have far-reaching consequences to today's investigations, but to the criminal justice system and even society as a whole: 'doing [attribution] poorly undermines a state's credibility, its effectiveness, and ultimately its liberty and its security' [19, p.4].

What is needed, according to US officials, are backdoors in encryption technologies to provide law-enforcement agencies authorized access to evidence [22]. This standpoint has been criticized, most notably by the academic world and private technology sector. Some bring forward the various encryption workarounds for law-enforcement to reveal an unencrypted version of a target's data that has been concealed by encryption [23]. Others argue that the debate is largely taking place without reference to the full picture as 'the "going dark" metaphor does not fully describe the future of the government's capacity to access the communications of suspected terrorists and criminals' [24, pp.3, 15]. Law-enforcement would have many substitutes to collect evidence in today's Information Age such as vast amounts of unencrypted metadata that were unavailable before criminals used widespread information technologies. Therefore, academics have suggested that this is in fact the golden age of surveillance [25]. The other side of that 'full picture of governments' capabilities' is, however, that cyber criminals also have many substitutes beyond encryption at their disposal for evading legitimate efforts of law-enforcement to collect evidence and conduct attribution [26].

The security practices of the Carbanak group
So what helped the Carbanak group to stay out of hands of law-enforcement for at least five years? Command-and-control servers (C&Cs) were located in multiple jurisdictions and only active for a short period of time, while secure deletion was applied to limit the amount of information on these C&Cs. These servers were rented from a criminal hosting provider (also known as bulletproof hoster), and credentials for the registration of these servers proved to be fake. Moreover, the group was located in China, Europe and Russia while making victims in Asia, Europe and North America. Indeed, formulating a joint investigative response by all affected jurisdictions was near to impossible in times of rising geopolitical tensions. Money mule handlers applied counter-observation techniques, while rumor had it diplomats were allegedly deployed to transfer cash. Notably, one might suspect that the cyber criminals also used encryption. Besides encrypted data in motion (read: secure communications on a data link and network layer), the fact is that the full extent of encryption usage by the group remained unknown to the cyber security community. The security practices were so good that law-enforcement never came close to the application layer of the other group members - read: seizure of their personal computers and the hypothetical encounter of encrypted data at rest.

1.1 Research Direction & Objectives

The Carbanak case suggests that i) cyber criminals apply security controls, ii) these controls deviate - at least, in the nature of their purpose - from law-abiding entities, and iii) these controls are affecting the effectiveness of legitimate responses. Yet a reversed security perspective, that we refer to in this study as *deviant security*, is largely absent from the literature as a topic in itself in several relevant disciplines. As visualized in Figure 1.1, deviant security has so far not been researched in a systematic and structured manner, and therefore we do not have a full picture of the protective practices of cyber criminals that are thwarting the legitimate investigations of law-enforcement agencies. The focus of the public debate is mostly on encryption usage for criminal purposes, but other deviant controls and their interconnectedness are largely known unknowns to both academics and legal practitioners.

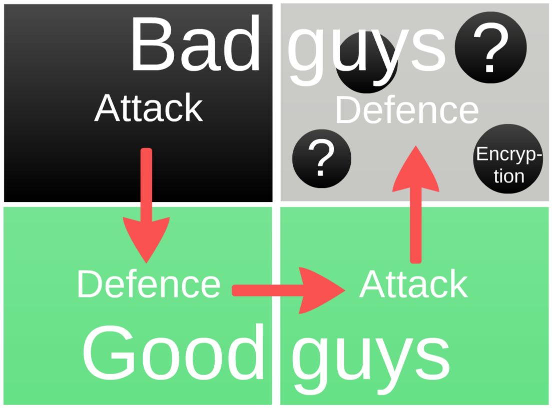


Figure 1.1: Besides defensive measures against attacks from bad guys, law-abiding entities might strike back by launching - amongst others - police investigations. In turn, cyber criminals have to defend themselves as well. While there is academic, corporate, media and political attention for attacks by cyber criminals and defences and attacks by law-abiding entities (read: known knowns), the security practices of cyber criminals are largely known unknowns.

Research direction Against this background, this study is organized around the following central research direction:

What are deviant security practices of cyber criminals?

Objectives Although cyber criminals are referent objects of security as well, current dominant security discourses do not explicitly name them as such: as entities that are apparently under attack and, therefore, in need of protection. As such, it remains the question what deviant security exactly entails, and when, where, how, why and by whom, it is applied. Fabian et al. state that:

> 'Unless we know what to secure, against whom, and to what extent, it is obviously very hard to construct a secure system or to make a substantial statement about its security' [27, p.7].

This statement is also very true for deviant security. Many scholars have stressed the importance of proving the need for expansion of investigative powers in the field of cyber crime [28][29][30][31]. Unless we know what cyber criminals secure, against whom, and to what extent, formulating effective offensive countermeasures is not only a challenge, but also comes at a cost. Ineffective responses - such as governmental requests for system backdoors - absorb scarce resources to identify few perpetrators, which subsequently decreases the security of all (potential) victims [32, p.289]. As cryptographer Bruce Schneier puts it, 'you can't build a [system] back door that only the good guys can walk through' and keeps the bad guys out [33]. For these reasons, the overall goal of this study is to:

- Present a new security paradigm, i.e., a first full picture on deviant security to an academic and legal practitioner audience.

The specific objectives in support of this overall goal are to:

- Describe and explain the technical computer security practices of cyber criminals; and

- Explore investigative responses against these protective practices.

1.2 Significance of Study

Because so little is still known about cyber crime and the public stakes are so high - intrusive investigative powers might affect the liberty of law-abiding citizens - scientifically collected data should prevail in the public debate above anecdotes or selective data provided by, for example, commercial parties [20, pp.124, 393]. Otherwise, we are indeed confusing the rhetoric with reality [34]. Deviant security practices have the ability to affect human rights when incident-driven measures are launched in response, only to show that 'something is being done', rather than evidence-based law and policy-making [13, pp.6, 9]. So any academic model on deviant security (in this study abbreviated to DevSec) should not only generate ideas for future, more in-depth research, but also connect to the world of legal practitioners, i.e., those legitimate threat agents that have a public mandate to attack the security of cyber criminals. Formulating comprehensive cyber security policies, evidence-based criminal procedure, and effective police investigations that stop and/or disrupt cyber crime is therefore very much the terminus for researching deviant security. An explicit framework capturing the multiple dimensions of deviant security practices will help academics and legal practitioners in liberal democracies governed by the rule of law to overcome the current effectiveness crisis in investigations. Thus, the study intends to sit between an academic and practitioner work. More specifically, the outcomes of this study aid:

- Prosecutors and law-enforcement officers, including data analysts and scientists, digital investigators and software developers, to conduct effective investigations. This study provides insights how to determine and identify suitable targets, how vulnerabilities of suspects can be exploited, and how multiple investigative outcomes can be delivered that go beyond attribution.

- Legislators to write evidence-based criminal procedural and substantive laws. More specifically, the findings help to understand which deviant security practices are criminalized in substantive law, and which practices are recognized as such in explanatory reports of procedural law. Additionally, the research extends our knowledge about the criminogenic aspects of criminal law.

- Policy makers to formulate comprehensive cyber security strategies that take the multifaceted nature of deviant security into consideration. This includes the geopolitical dimensions and key players in the cyber criminal and cyber security communities, and related responses such as investments in resources and fundamental rights and freedoms.
- Technical computer security researchers, social scientists and legal scholars to understand the socio-technical-legal interplay between deviant security practices and investigative responses.

1.3 Approach

This study researches the security practices of cyber criminals. The definition of deviant security is (further explained in detail in Section 5.1):

> all technical computer security controls of natural and legal persons who are criminally liable for the commission of crime, in order to protect the criminal and his/her crimes.

Their protective practices are described and understood from a technical, or in other words, computer science perspective on security (known as technical computer security [30]). Permission was given by relevant academic and government authorities to have access to confidential secondary data sources from police investigations on predominantly financially-driven cyber crimes, while a total of five years was spent within the cyber security community. Used data sources relate to those who conduct deviant security as well as those who are confronted by it, respectively participants from the cyber criminal and cyber security community. Grounded Theory is subsequently used to generate high abstract categories from the encountered technical computer security policies and mechanisms, while microeconomics is applied to explain the encountered practices. Grounded Theory and microeconomics are also used to explore outcomes that will benefit public policy, criminal procedure and police investigations, and as such affect the protection of cyber criminals. This legal end point, in combination with the study's legal starting point - i.e., a problem witnessed by law-enforcement agencies - shows the multidisciplinary nature of researching deviant security. In other words, social science methods and techniques are used to research the computer science understanding of security of those individuals who trespassed substantive law.

1.4 Novel Contributions

The main contribution of this research project is to present, to the best of our knowledge, the first structured, systematic and multidisciplinary study on the deviant security practices of cyber criminals and investigative responses. The final result is a model that has conceptual density, explanatory power and durability over time, based on - amongst other things - unprecedented access to unique data sets. In addressing the objectives outlined above, this thesis further makes the following novel contributions that include but are not limited to:

- Formal definitions for modus operandi and deviant security practices;
- The introduction and development of the economics of deviant security, and the outline of other socio-technical(-legal) disciplines such as the anthropology, linguistics and psychology of deviant security, and empirical legal scholarship on deviant security;
- Taxonomies for criminal assets, deception, distrust and phases of international collaboration between law-enforcement agencies;
- New (deviant) security-related concepts like bulletproof connectivity providers, double whammy effect of deviant security, intercultural communicative security, points of attack linkage and inherent (i.e., unavoidable) weaknesses;
- The application of existing technical computer security and microeconomic concepts to the worlds of cyber criminals and legal practitioners to understand the protection of crime and police investigations.

1.5 Outline of Study

The study has the following structure:

- *Part I Literature Review:*
  - *Chapter 2 - Current 'Good Guy' Perspectives on Security* starts with an overview of our current understanding on security in which law-abiding entities are referent objects. Using an adapted security process cycle of the Common Criteria for Information Technology Security Evaluation, this chapter shows how a computer science perspective on security (i.e., technical computer security) and a border-centric and borderless socio-legal view on cyber security and cyber crimes each have their own referent objects, threat agents, attacks, vulnerabilities, risks, assets and countermeasures.
  - *Chapter 3 - Touching upon Security Controls of Cyber Criminals* uses the security process cycle again to review deviant security-related literature from computer science, more specifically anti-forensics, botnet protection, authorship analysis and attacker economics. A literature review on relevant social science studies provides input for a new definition for modus operandi that emphasizes the need for the criminal to protect him/herself and his/her crimes. A review on legal scholarship concludes that police investigations breach deviant security, criminal law is essentially disruptive, and investigative powers should be seen as legitimate attacks by law-enforcement agencies.
- *Part II Methodology:*

    - *Chapter 4 - A Multidisciplinary Approach for Deviant Security* explains how and why the computer science understanding of technical computer security concepts is central in this study, but enriched with social science and legal scholarship. More specifically, the chapter points out why the qualitative methodology of Grounded Theory is used to describe, and microeconomics to explain, the deviant security practices of predominantly profit-driven computer-focused criminals in the Information Age. The chapter further elaborates on used secondary data sources from participants of the cyber criminal and cyber security community, and associated limitations and ethical issues.

- *Part III Research Findings:*

    - *Chapter 5 - What? - Basic Qualities of Deviant Security; Chapter 6 - Who? - Interactive Qualities of Deviant Security;* and *Chapter 7 - When & Where? - Temporal-Spatial Qualities of Deviant Security*, present the first full picture of deviant security practices. Amongst others, the basic normative and empirical qualities are described and explained, more specifically definition, meaning, provision, function and form of deviant security. The interactive qualities consist of a description of referent objects, providers and threat agents of deviant security, why these key players are nodes in intertwined networks and face information asymmetries as a vulnerability, and how deception, trust and distrust work as deviant security controls. The temporal-spatial qualities of deviant security are categorized as countermeasures against data volatility and retention, intercultural communicative security, distribution as a countermeasure, and physical deviant security.

    - *Chapter 8 - Investigative Responses Against Deviant Security* presents investigative approaches against deviant security that legal practitioners could explore. Based on the findings of the previous chapters and additional empirical research, this chapter explains why investigations on profit-driven computer-focused crimes should become security-driven, regard Internet as a global public good and provide human security. Within that normative framework, investigations should be developed following a public service model with multiple outcomes, while technical harmonization between law-enforcement agencies is needed to fix a broken global investigation system. Lastly, this study indicates which profit-driven computer-focused crimes should be targeted by law-enforcement agencies, and how to approach these investigations.

- *Part IV - Conclusions:*

    - Because most chapters have interim conclusions and discussions, *Chapter 9 - The Outlook of Deviant Security* finalizes this study by reiterating the thesis objectives, filling in the security process cycle with cyber criminals as referent objects, and summarizing the research findings as well as providing the reader some general directions for future academic work.

A last remark is that *italic* characters are not only an invitation to focus the reader's attention on specific concepts, but are also used for non-English words.

Part I

Literature Review

Chapter 2

Current ‘Good Guy’ Perspectives on Security

In order to describe and explain the new security paradigm of deviant security, we first have to understand what *current* academic and practitioners’ perspectives are on security as an ongoing process. Literature reviews are subsequently conducted on the computer science understanding of technical computer security and the legal and social science understanding of cyber security and cyber crimes. As such, this chapter fulfills three purposes for the overall study, namely to i) point out that current studies evolve around law-abiding referent objects - ‘good guys’ - who are threatened in their security by law-breaking threat agents, i.e., ‘bad guys’; ii) explain why the computer science understanding of technical computer security is used to research the deviant security practices of cyber criminals, and why the legal and social science understanding of cyber security and cyber crimes is applied to explore appropriate responses against these practices; and iii) familiarize the reader with the security terminology and language that is used throughout this study .

Good guys and bad guys?
The labels good guys and bad guys are a simplification of reality, but are used by this study, other studies and the larger cyber security community to make an argument (see for example [35, p.197][36, p.xxviii][37, p.226][13, p.6]). This study acknowledges that society cannot simply be divided into good guys and bad guys, and that criminals are not the only cause of crime. The nature and extent of the commission of crime depends on many factors, and is not proportional to the number of good guys and bad guys [38, p.1]. As Section 2.3 explains, states and businesses may also be the bad guys, and become threat agents to the security of law-abiding citizens [39]. The same reasoning about the commission of crime can be extended to security of crime. Cyber criminals are not solely responsible for the protection of crime. The security of cyber criminals also depends on various other factors such as micro, meso and macro conditions. In fact, the way we view and react to the bad guy cyber criminals may be rooted in cultural factors - such as popular media representation of computer hackers - rather than scientific evidence [40].

2.1 Security as an Ongoing Process

This chapter begins by explaining an important feature of this study: the distinction between the computer science understanding of technical computer security and the social science and legal understanding of cyber security and cyber crimes. Despite their differences, the two views also have an overlap. They both regard security as an ongoing process, a cycle that consists of six security components derived from the general model of the Common Criteria for Information Technology Security Evaluation - an internationally recognized standard for technical computer security products [41, pp.40-43], and depicted in Figure 2.1.

Distinguishing technical computer security from cyber security Security is a 'promiscuous concept', 'slippery and contested term', and 'too big an idea' to be left alone to a single academic discipline [31, pp.3, 9-10]. Understanding security traditionally involves disciplines such as international relations, public international law and war studies, and further includes the social sciences, especially related to crime control such as security studies and criminology [31, p.1-3][42, p.xi][43]. Due to dominant role of information technology (IT) in present-day society [44][45][46], computer science (CS) has entered the security arena as well with the discipline of technical computer security and its influence on the social science and legal understanding of cyber security [30]. To describe and understand these new security objects of technical computer security and cyber security [47, p.3], scholars from both computer and social science conduct security analyses that take a closer look at the practices of those who 'do' security [48, pp.21-47]. Security is - amongst others - a social practice and continuing activity of those involved [31, p.21], which means that security is a social process of protecting *us* from *them*, i.e., the 'threatening Other' [49, p.4][50, p.54]. It is not merely a technical phenomenon, but embedded in social context; thus very much a social product as well [51, pp.320,338]. The non-discursive and discursive practices of security actors such as security professionals, and their interactions with criminals and crime, shed light on what security encompasses [4, p.1165][52, pp.98-100]. The security terminology in computer science literature is often similar to the language of these social scientists [5, p.5]. When the shared language between both disciplines is identified, a process cycle emerges that consists of referent objects, threat agents, threats, vulnerabilities, risks, valuables and countermeasures (see next paragraph). This socio-technical security cycle is used in Sections 2.2 and 2.3 to determine what the specific meanings of these components are in respectively technical computer security and cyber security. Section 2.4 concludes that a security analysis on the deviant security practices of cyber criminals should incorporate insights from both discourses.

The security process cycle Firstly, security analyses are written from the perspective of a certain entity that is in need of security. While most computer science literature implicitly assumes this recipient of security (Fabian refers to recipients of security as the security stakeholder [27, p.8]), security studies and criminology explicitly refer to this entity as the *referent object*. Referent objects are entities that are (existentially) threatened and have therefore a legitimate claim for survival ([48, pp.36-37]). Subsequently, this *us* must be protected from a certain *them*: the *threat agent*, a term mainly found in computer science [53][27][54]. This threat agent gives rise to a *threat* (both disciplines, e.g., [43][41]). Intentional threats - the focus of this study, as compared to accidents, failures and mistakes - that become real are called *attacks* (both disciplines [55][34][36]. The attack may exploit a *vulnerability* (both disciplines, e.g., [27, p.13][43, pp.53,269][56, p.408]). The possible exploitation of a vulnerability leads to a *risk* (both disciplines, [43][27][57]) that *valuables* or *assets* will be damaged (both disciplines, [58, p.20][59][54]). This causes an instance of being exposed to losses, and therefore *countermeasures*, *safeguards* or *controls* have to be installed to mitigate the potential risk and protect the assets (both disciplines, [27][4][34][41]). In turn, these countermeasures of the referent object affect the threat agents as well which makes security very much a social process. The interplay between entities (us versus them) and their offensive and defensive activities affect the security of all key players involved [35, pp.234-236], whether law-breaking or law-abiding/enforcing. Security is therefore understood in this study as an ongoing, circular process as depicted in Figure 2.1. The next sections show that although the security terminology of the components is similar in both disciplines, they indeed have very specific meanings [5, p.5], based on which referent object is chosen. We therefore add referent object as a new component to the general model of the Common Criteria for Information Technology Security Evaluation, and put it at the centre of the security process cycle.

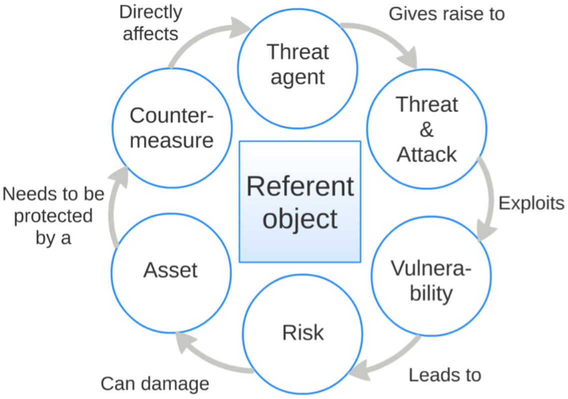


Figure 2.1: The relationship between various components of the security process cycle. The cycle is based on the general model of the Common Criteria for Information Technology Security Evaluation [41, pp.40-43][59, p.27], and adapted by creating the new component of *referent object*, adding the term *attack* to the existing component *threat*, and removing the component *exposure*.

2.2 Current Perspective on Technical Computer Security

Considerable consensus exists in computer science literature on what technical computer security encompasses. These studies are written by academics and computer experts who are concerned about malicious attacks on the confidentiality, integrity and availability of computing systems and information of law-abiding entities. The terminology of this perspective is very much the language of those with advanced technical academic and/or skills background, such as computer scientists, digital investigators, (information) security officers and private security researchers, but also cyber criminals. As a consequence, technical computer security language is found in - amongst others - academic papers, court documents, cyber threat analyses and indeed, postings on cyber criminal fora. This perspective devotes less attention to understand the behavior of those who try to breach technical computer security, and place their actions within criminal law.

Referent objects, threat agents, attacks & vulnerabilities The computer science literature addresses technical computer security [30, p.63], i.e,. the sum of security areas such as communications [36][53], computer [60][36], information [61][53], Internet [62], and network security [63][64]. The common denominator in these different but related fields (and what distinguishes security in computer science from other disciplines such as social sciences) is the centrality of technology [62, p.2]. The *referent objects* of security in computer science literature are personal, business or government users of commercial, military or public computing systems [27, p.11][5, pp.7-8][65, p.4][36, pp.4-8]. The *threat agents* of these computer users are those who - intentionally or unintentionally - breach technical computer security. The literature generally does not use criminological typologies or legal categories, nor comprehensively elaborate on offender characteristics, but commonly refer to them as ‘computer criminals’. Those include ‘amateurs’, ‘career criminals’, ‘crackers/malicious hackers’ and ‘terrorists’ [53][54]; and ‘agents of hostile governments or organisations’, ‘corrupt insiders’ and ‘vandals’ [66, p.7]. Their *threats* and *attacks* - also known as attack vectors or exploits - are labeled on a high level of abstraction in technical terms of ‘interception, interruption, modification, and fabrication’ [54][67, p.378], and in terms with a more legal connotation such as ‘espionage’ (e.g., illegal access and interception), ‘theft’ (computer-related forgery and fraud), and ‘sabotage and vandalism’ (data and system interference) [53, p.44]. On a lower level of abstraction, attacks exploit vulnerabilities in the security of computing systems of the referent object [65, p.6][54], and are labelled with technical classifications such as malicious software (also known as malware such as Trojan horses, viruses and worms), hoaxes, back doors, password cracks, spoofing or social engineering [64, pp.65-74]. *Vulnerabilities* consist of software, hardware, procedural, and - to a lesser extent - human weaknesses to enter the referent object’s computing system and have unauthorized (thus unlawful) access to assets and/or make assets unavailable [68, p.54].

Risks, assets & countermeasures The probability that the system will not be able to enforce its security policy and for harm to occur is called *risk* [54][65, p.6]. Referent objects generally perform quantifiable risk assessments to determine the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact [68, pp.54, 85-89]. The business impact is objective and measurable, and expressed in financial losses [69]. For example, there might be reputation damage after a security breach in a company which is shown by a drop on the stock exchange. The exploitation of vulnerabilities may damage the confidentiality, integrity and availability of *assets* of the security recipient (also called the CIA triad : a fundamental concept within technical computer security [64, p.16][66, p.2]). Valuables of any computer system are its hardware, software, data [54][67, p.378] and users [53, p.9]. For instance, misconfigured web applications might not validate user input before using it to query a relational database in web sites. A successful structured language language (SQL) injection puts actual database commands into the input fields to have unauthorized access to data which may result in the loss (availability), public leak (confidentiality) or alteration (integrity) of valuables such as user IDs and passwords [59, p.1163][53, p.79]. To prevent such an exposure from happening, referent objects put *countermeasures* in place to control any potential vulnerability and protect assets. The proposed controls consist of security policies and security mechanisms. The policies are a description of security requirements, and prescribe which actions are allowed by which entities in a system. This security strategy is subsequently enforced by mostly technical security mechanisms such as access controls and encryption, but may also consist of administrative and physical security controls [36, p.11][67, p.379]. Security tradeoffs are made between the costs of applying security countermeasures and the benefits realized from the operation of secured, available systems [53, p.119], and are expressed in positive economic statements about what occurred or will occur (as compared to normative economic statements which involves value judgements [70, pp.7-8]). The controls may further be subjected to industry standards [57, pp.34-35], and increasingly civil and even criminal liability as well (because of due diligence and due care, respectively the assurance that the responsible legal and natural persons did everything to understand threats, and the assurance that he/she took all necessary countermeasures to prevent or respond to these threats [36, pp.375, 388][59, pp.1022-1023]). The key actors of these policies and mechanisms are predominantly computer experts, such as system administrators, and the private security industry like antivirus vendors [5, p.7].

2.3 Current Perspectives on Cyber Security & Cyber Crimes

Cyber security and cyber crimes are terms articulated in a range of legal, policy and other texts of academics, businesses, governments and media. The documents are, compared to computer science literature, more ambiguous when it comes to filling in the various components of the security analysis. The first section explains why not only literature about cyber security is reviewed, but also literature about cyber crimes that do not affect cyber security, such as the distribution of child sexual abuse material (CSAM - also known by the legal term of child pornography, see article 9 of the Budapest Convention of the Council of Europe). The security analysis of the second section shows that the current border-centric view on cyber security/cyber crime discourse is more extensive in scope and involves more actors than the technical computer security discourse. Law seems more dominant in the cyber security/cyber crime discourse in which substantive law defines threat agents, threats and attacks, and procedural law governs countermeasures by law-enforcement agencies. The last section describes an alternative borderless view on cyber security and cyber crime derived from political science and security studies in which the threat agents are not cyber criminals, but states and the private sector to the security of citizens (which underlines that the distinction between 'bad' cyber criminals, and 'good' states, businesses and citizens, is indeed oversimplified).

2.3.1 Why Cyber Crime is (not) Cyber Security

Social sciences - most notably criminology and security studies - have been relatively slow in studying the reasoning of the cyber security debate. A coherent body of literature on cyber security seems therefore absent in social sciences [5, pp.2-3]. There is little agreement among academics and policy makers what cyber security exactly entails, and there is little on what cyber security does not cover [71, pp.587, 591, 593]. Cyber security generally includes the protection of the totality of national critical infrastructures (NCI): those assets and systems necessary to preserve national security [58][5, pp.7-8][72, p.54]. As such, cyber security links the above mentioned technical computer security to traditional notions of national interests [30, pp.63-64]. Yet cyber security has a wider scope and different key actors than the computer scientific perspective on security such as the use of the military, intelligence services and law-enforcement agencies - i.e., mandated breachers of deviant security - as countermeasures [55, p.156], see Figure 2.2. The focus in this section is on i) the cyber criminal attacks that affect the national critical infrastructure (i.e., risks to cyber space), and ii) crimes that involve the use of computer technology but are not part of the cyber security discourse because they are not directly related to the protection of national critical infrastructure. The associated attacks within this discourse include crimes that pose a risk through cyber space, such as but not limited to the distribution of child sexual abusive material [73, p.660][58].

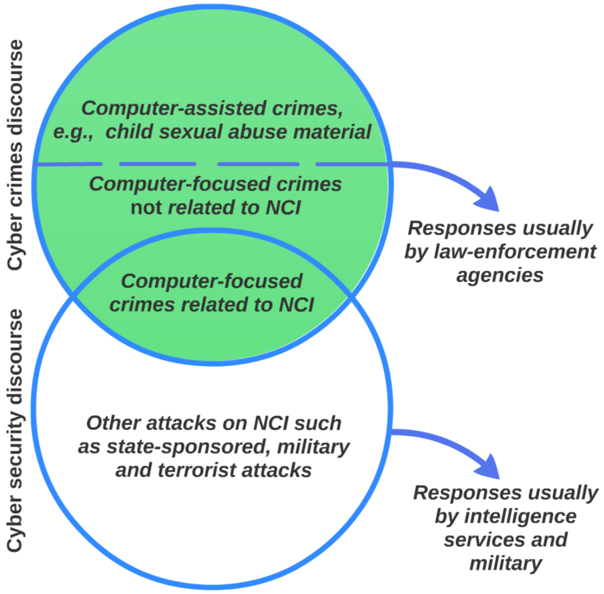

Cyber crimes discourse
Cyber security discourse
Computer-assisted crimes, e.g., child sexual abuse material
Computer-focused crimes not related to NCI
Computer-focused crimes related to NCI
Other attacks on NCI such as state-sponsored, military and terrorist attacks
Responses usually by law-enforcement agencies
Responses usually by intelligence services and military

Figure 2.2: The Venn-diagram shows the differences and overlap between the cyber security and cyber crime discourses in the social science literature. The focus of this study is highlighted in green. The terms computer-assisted and computer-focused crimes are explained in the next section.

The distinction between the cyber security and cyber crime discourses is, however, blurred. According to Dunn Cavelty, the two discourses are no longer separate, but have become one and the same:

> 'With the growth and spreading of computer networks into more and more aspects of life, the object of protection changed. Whereas it had previously consisted of limited government networks, it now compassed the whole of society' [55, p.159].

For example, it is argued that cyber security conceptualizations of the European Union (EU) are painted in 'any colour they like', including child sexual abusive material and piracy [74], see Figure 2.3. For this reason, and because the components of a security analysis may also apply on cyber crimes that do not affect critical information infrastructure (such as the production and distribution of child sexual abusive material), the cyber crime discourse is added to the security analyses of the next paragraphs.

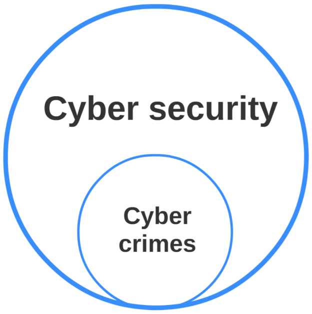


Figure 2.3: The Venn-diagram shows the incorporation of cyber crimes into the cyber security discourse. In this conceptualization, all cyber crimes, including the possession of CSAM and intellectual property violations, are considered cyber security issues.

2.3.2 Border-Centric View on Cyber Security & Cyber Crimes

Social science scholars (especially criminologists and sociologists) and legal scholars have analyzed the criminal practices of cyber criminals, and the responses of legislators, policy makers and the private sector. They take what this study calls a *border-centric view* on cyber security and cyber crimes as all entities within a certain jurisdiction are regarded as referent objects of security.

Referent objects, threat agents & attacks As mentioned above, the distinction between the cyber security and cyber crime discourses is blurred. Because technological infrastructures provide the way of life that characterizes today's societies, and because the well-being of individual and corporate actors is often regarded as equal in importance to the well-being of the state [75, pp.10-11][5, p.7], *referent objects* - labeled as (potential) victims of cyber attacks [29] - are not restricted to computer users, but include collective, macro-level entities within society that relate to national interests [30, p.69], namely the state, corporate sector and general public. Classifications on threats and attacks by threat agents in both discourses evolves around the role that technology plays in the commission of crime, namely object, instrument and environment of crime [76, p.738]. In the cyber security discourse, *threats and attacks* fall in three socio-technical categories, namely i) the use of networked computers as a medium or staging ground for antisocial, disruptive, or dangerous organizations and communications, ii) threats/attacks against critical societal infrastructures, and iii) threats/attacks against the networked information system itself [30, p.64]. These attacks are executed by a range of malicious *threat agents* such as hacktivists, hostile states, disgruntled employees, professional criminals, terrorists, and thrill seekers [77]. The cyber crime discourse follows a more clear *criminological* classification, and distinguishes computer-oriented/focused criminals and offenses such as unauthorized hacking from computer-assisted criminals and offenses such as the production, distribution and possession of child sexual abusive material [78, pp.3-4][28, pp.10-11][79, pp.3-5][29, pp.527-538] (for more criminological classifications, see [80][81, pp.7-8] and the text box below). The Convention of Budapest of the Council of Europe (also known as the Cybercrime Convention) is considered the main international *legal* instrument in fighting cyber crime [57][82, p.215], and categorizes cyber crimes as offenses against the confidentiality, integrity and availability of computer data and systems; computer-related offenses (fraud and forgery); and content-related offenses of unlawful production or distribution of child sexual abusive material by use of computer systems (see also [34, pp.49-50][83, p.52]).

Computer-focused, assisted and enabled crimes
This study distinguishes three types of cyber crime. The first are *computer-focused crimes* (also known as computer-oriented crimes [84]). These malicious acts could not exist without information technologies, and are, as such, 'new crimes, new tools' like malware, botnets and distributed denial-of-service (DDoS) attacks. *Computer-assisted crimes* are those acts that could occur in the physical world but can also be replaced by means of IT. Examples are child sexual abusive material, forgery, harassment and identity fraud. In the past, child abusive material was on print, but nowadays predominantly resides as data files on computer systems. Lastly, *computer-enabled crimes* are analogue acts that can only exist physically, yet parts of the modus operandi of these traditional crimes are supported by IT. While illegal substances and fire arms are offered for sale on online cryptomarkets - also called Dark Markets - and paid for by cryptocurrencies, the drugs themselves cannot be virtually consumed, nor can machine guns be shipped and used in a digital manner.

Vulnerabilities, risks & assets Similar to technical computer security, these cyber threats exploit *vulnerabilities* of the referent objects. Besides technical weaknesses, considerable attention is also paid to human weaknesses. Producers of child sexual abusive material may target toddlers and babies whom are vulnerable because they are defenseless against the abuse, and unable to disclose the abuse [85, p.76]. Groomers may exploit technical vulnerabilities to install remote access tools to spy on their victims. The sum of both technical and human weaknesses may lead to the conclusion that certain groups of referent objects are vulnerable, hence labels as vulnerable children [86, p.96] or vulnerable citizens [57, p.55]. The possible exploitation of a vulnerability leads to a *risk* that valuables of referent objects are harmed. Because the cyber security community has since long acknowledged that absolute security is impossible [55, p.161], public and private parties conduct risk assessments. These assessments help to determine the likelihood of a threat agent taking advantage of a vulnerability by calculating factors such as the propagation and longevity of each type of attack and the corresponding impact [57, p.13]. The impact goes beyond the scope of the technical cyber security perspective in which only business impact expressed in financial losses is incorporated. It may include losses that are not easily quantified such as emotional harm [87][57, p.48], and subjective issues such as perceived security feelings of (potential) victims [88][31, pp.16-19]. So risk in the cyber security and cyber crime discourses encompasses objective and subjective damages, expressed both qualitatively and quantitatively.

Compared to the computer science literature, *valuables* in the cyber security and cyber crime discourses are more broadly defined and normatively enriched [62, p.2]. They basically include everything that effects society's survival and well-being at large. In cyber security, scholars include 'cyberspace and critical infrastructure' [58, p.20], 'national economies' [17, p.659], 'the stability and order of a society necessary to survive' [73, p.668], and 'public interest and order, property or the person' [89]. In the cyber crime discourse, valuables that are affected by cyber crimes also include the emotional, physical and mental well-being of individuals [87]. For example, the rationale behind criminalizing child abusive material is the protection of the child, because the production and distribution of the material harms the well-being of the child, even after the physical abuse has stopped [85, pp.49-50].

Countermeasures There seems little consensus what *countermeasures* exactly encompasses, and what the roles and responsibilities are of those who should provide these safeguards. It is, however, apparent that proposed and implemented controls in the cyber security and cyber crime discourses have a wider scope and involve other actors than in the technical computer security discourse. Because liberal democratic states have limited control over the Internet infrastructure [90][34, pp.210-211], responsibilities for security are distributed [31, pp.49-66][91], especially to the corporate sector [55, pp.160-161][58, p.18][92][73]. Simultaneously, the cyber security and cyber crime discourses still place great control in the hands of centralized public authorities, and rely more on strategies that involve scrutiny, individual accountability, transparency and identifiability [30, pp.71-72]. Because security is about survival and well-being, the use of extraordinary measures and the legitimized use of force by states are justified to control threats [48, p.21]. Where technical computer security controls are less concerned with identifying and stopping attackers before they act, and more focused on strengthening protections for potential targets, much attention is paid in the cyber security and cyber crime discourses in determining the identity and intent of the malicious actor. Criminal law is used for that purpose and as a countermeasure as law defines misdemeanor and enables arrest and prosecution [55, p.160][5, p.10][71, p.588][93, pp.727-728]. Thus, countermeasures against cyber threats from both discourses may be divided in a broad range of preventative measures (safeguards before an offense has happened, such as increasing awareness through education and surveillance) and reactive measures (controls after the offense occurred, such as police investigation and prosecution) by states, businesses and individuals [29, pp.542-543][34, pp.186-192][93, pp.725-729]. Security tradeoffs are both positive and normative. An example of the former are policy decisions about focusing police investigations on either the bulk of easily identifiable viewers of CSAM, or the small group of producers of abusive material which is considerably harder to identify [85, p.168]. Normative tradeoffs are made when countermeasures (such as investigations) affect legal rights and related concepts of suspects and the general public, such as privacy versus security [94][95].

2.3.3 Borderless View on Cyber Security & Cyber Crimes

A border-centric view on cyber security and cyber crimes implies there is also a *borderless view* with other referent objects of security. Scholars from criminology and security studies - especially Dunn Cavelty, Hansen and Nissenbaum from the Copenhagen School, and Loader, Walker and Zedner from the Oxford School, see [96] - have also analyzed the practices of legislators, policy makers and the private sector related to respectively security and information technology, and cyber security and cyber crimes (for an overview of other schools and their approaches to security, see [43, pp.35-38]). From their view, citizens should be referent objects of security, regardless of location and/or nationality.

Referent objects, threat agents, threats and attacks These scholars with a borderless view on cyber security and cyber crime conclude that there is too much emphasis on states and businesses as *referent objects* of security at the expense of citizens within and outside national borders. This emphasis can cause the general public to feel threatened rather than protected by the state and/or the private sector. Instead, the general public ought to be the basic referent objects of security [97][98, pp.17-18], as governments and the private security industry may become *threat agents* of the general public, especially as governments are clients and pilot laboratories for much of the security industry [99, pp.46-47]. *Threats* - the potential dangers that these threat agents pose to the security of citizens - are the process of securitization and the commodification of security. Securitization is the (undemocratically) political process in which events, issues and/or groups are framed as potential security problems to enforce extraordinary powers [48, pp.23-26][100], much what happens, according to some researchers, in the going dark debate on encryption usage [101]. The launch of extraordinary powers includes, for example, indiscriminate mass surveillance in which all citizens are seen as potential suspects [102, pp.458-464]. The threat of commodification of security means that security becomes a private good, thus a tradable commodity for a happy few [103][104]. In short, both securitization and commodification make security an exclusive private good, rather than an inclusive public good.

Vulnerabilities, risks, valuables and controls The threat agents exploit human *vulnerabilities* such as the citizens' fear of crime and terrorism [98, p.2], or the inability of citizens to exercise democratic control over the threat agents [105]. These threats lead to a *risk* that citizens' valuables are damaged. Scholars criticize the perception of risk as defined by the border-centric view on cyber security and cyber crimes [75, p.144]. Absolute security is unattainable and the limitless pursuit for security only benefits the private security industry, while legislating for uncertainty leads to indiscriminate mass surveillance and the extension of criminal liability [31, pp.126-134, 145, 151-155]. Objective security assessments - whether a threat is real - are beyond means of analysis. Rather, securitization is intersubjective and socially constructed [48, pp.29-35]. *Valuables* of citizens are public access to security [106, p.162], fundamental/human rights [107, pp.55-56], democratic principles [98, p.2], and/or civil liberties [31, p.2]. To prevent harm to these valuables, scholars suggest *controls* such as desecuritization (i.e., finding ways to politicize issues in non-security ways [48, p.29][4]), and civilized security (i.e., security as a 'thick' public global good provided by states that, according to Loader, must themselves be civilized - made safe by and for inclusive democracy - to release the civilizing potential of security [98, pp.4-8]). Some scholars are even 'against security' at all [108]. These controls are not put forward as mutually exclusive tradeoffs. On the contrary, security is reinforced by normative conceptions of, for example, privacy and liberty. Thus, more privacy for citizens will the increase their security against the threats of businesses, criminals and governments [97].

Table 2.1: A summary of the various security discourses.

Security analysis component	**Technical Computer Security**	**Border-Centric View on Cyber Security & Cyber Crimes**	**Borderless View on Cyber Security & Cyber Crimes**
Referent objects	Individual entities: computer users	Collective entities: the state, private sector and general public within a certain jurisdiction	Collective entities: citizens
Threat Agents	Those who breach technical computer security	Those who intentionally trespass substantive law	States and private security industry
Threats & Attacks	Technical classifications from computer science: attack vectors and exploits	Legal and social-science classifications from substantive law and criminology: computer-assisted and computer-focused offenses	Social-science classifications from security studies: commodification of security and securitization
Vulnerabilities	More emphasis on technical than human weaknesses	Emphasis on both technical and human weaknesses	Emphasis on human weaknesses
Risk & expressions	Quantitative risks expressed as objective statements	Quantitative and qualitative risks, expressed as objective and subjective statements	Qualitative risks, expressed as subjective statements
Assets	Hardware, software, data and their users	Everything related to the well-being of society at large	Human rights, especially privacy
Safeguards & expressions	Technical computer security policies and mechanisms of a predominantly preventive and detective nature, executed by computer experts; expressed as positive statements	Preventative and repressive interventions distributed to - amongst others - law-enforcement agencies (procedural law); expressed as positive and normative statements	Desecuritization by politicians and civil society; expressed as normative statements

2.4 Interim Conclusion and Discussion

Although current security analyses on technical computer security and cyber security/crimes have different referent objects, threat agents, threats, vulnerabilities, risks, valuables and countermeasures, both are written from the perspective of good guy referent objects who are threatened by attacks from bad guy threat agents. As summarized in Table 2.1, the good guys protect their valuables against malicious acts of these threat agents. The law-abiding entities are portrayed as (potential) victims who are predominantly on the defensive side, while the bad guys are portrayed as malicious attackers who are only on the offensive side. The assets of these referent objects - states, businesses and citizens - are legitimate, and preventative and reactive safeguards comply with industry standards or public law. The bad guy cyber criminals follow the opposite direction. They are defined as threat agents because of their intentional trespassing of substantive laws, and their attacks do not comply with any public law or industry standard.

One of the countermeasures within the cyber security and cyber crime discourses are investigations by law-enforcement agencies. Their legal actions focus on identifying cyber criminals and gathering evidence about criminal activities. This means that cyber criminals are in need of security as well to avoid arrest and prosecution. So besides private, public and state security, there is also deviant security, namely: the security controls of criminals. Nonetheless, current security analyses do not take cyber criminals as referent objects of security. No academic studies from both discourses are found that explicitly ask what their threat agents, threats, vulnerabilities, risks, valuables and countermeasures are. In other words, there is a research opportunity to apply a reversed security perspective which combines components of both technical computer security and cyber security/cyber crime discourses.

In this reversed security perspective as depicted in Figure 2.4, the referent objects are the threat agents of the cyber security/cyber crime discourse, more specifically computer-focused criminals - e.g., criminal hackers who exploit vulnerabilities in the security of law-abiding entities - as well as computer-assisted criminals like viewers and possessors of CSAM who usually do not have to breach any security system to commit their crimes. Such a perspective further takes a look at the cyber criminals' technical computer security policies and mechanisms that protect computing systems, software, data and their malafide users. The focus on finding and understanding both technical and human vulnerabilities is derived from both discourses. The same goes for identifying objective and subjective risks and related cost-benefit analyses such as deviant security tradeoffs. This deviant risk analysis should initially be expressed in a qualitative matter as a full picture on deviant security is currently absent. Therefore, qualitative research first has to identify, construct and categorize protective practices of cyber criminals, before more quantitative approaches can be conducted. These insights will benefit the cyber criminals' threat agents and attacks as defined by the cyber security/cyber crime discourses, namely: law-enforcement practitioners and their investigations that serve the general public and operate within the legal boundaries of democratic states governed by the rule of law.

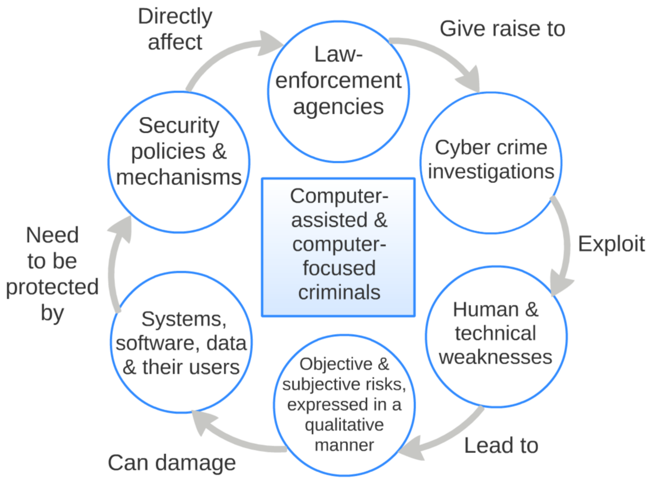

Directly affect
Law-enforcement agencies
Give raise to
Security policies & mechanisms
Cyber crime investigations
Computer-assisted & computer-focused criminals
Need to be protected by
Exploit
Systems, software, data & their users
Human & technical weaknesses
Objective & subjective risks, expressed in a qualitative manner
Can damage
Lead to

Figure 2.4: The components *Computer-assisted & computer-focused criminals*, *Law-enforcement agencies* and *Cyber crime investigations* are derived from the cyber security/cyber crime discourses. The components *Systems, software, data & their users* and *Security policies & mechanisms* are derived from the technical computer security discourse. The two components about weaknesses and risks are derived from both technical computer security and cyber security and cyber crime discourses.

Chapter 3

Touching upon Security Controls of Cyber Criminals

Although deviant security is not a well-identified domain in the academic literature, scholars and industry experts have discussed different aspects of security controls of cyber criminals. The empirical foundations for the tenets of this study are therefore already largely in place. This chapter uses the security process cycle to structure existing security research literature in computer science and engineering that touch upon the controls of cyber criminals. Deviant security perspectives are sometimes adopted in the literature, yet some potential areas of research are left unexplored and/or would benefit from an explicitly deviant security approach. The chapter then considers research in social science and legal scholarship respectively, particularly those studies that focus on understanding how the security of cyber criminals affects legitimate policing activity. This review is indeed not exhaustive and only discusses literature that relates to social processes of deviant security *practices* (compared to more psychological approaches that focus on cyber criminals' individual experiences about security). However, besides other purposes of literature reviews like identifying knowledge gaps [109, p.55], the goal of this chapter is especially to i) point out that cyber criminals probably have many more threat agents, threats, vulnerabilities, risks, valuables and countermeasures than the reviewed literature considers; ii) fine-tune the methodological direction of this study (Chapter 4); and iii) identify content area, themes and foci for the normative and empirical research part of this study (Part III). In short, these findings indicate that deviant security and appropriate investigative responses are challenging but promising fields of study, that will benefit from a more multidisciplinary approach to develop a comprehensive understanding of what deviant security exactly entails, and when, where, how, why and by whom, it is applied.

Extensive research on the security of traditional criminals is absent as well
There are very few studies that explicitly take cyber criminals as referent objects of security. Notable studies are, for example, Van Hardeveld et al. who explored the predominantly technical tools of anonymity used by carders - e.g., cryptocurrency mixers, remote desktop protocol, Tor and VPNs - and in a second study types of operational security by cyber criminals in general, and used as data sources respectively carder tutorials and expert interviews [110][111]. Sundaresan et al. researched the network behavior of cyber criminal forum members, exploited several technical vulnerabilities and provided their likely locations, work habits and other dynamics [112]. Yet these studies are either of a respectively very explorative or specific (i.e., technical) nature. Studies about the security of traditional criminals do not offer a helping hand either. There are academic papers within social science that directly refer to the security of traditional (i.e., offline) covert organizations, such as terrorist (e.g., Al-Qaeda) and criminal networks (e.g., Italian mafia). These scholars highlight security related issues such as secrecy and trust, and apply social network analysis and game theory to describe, explain and predict the security tradeoffs that terrorists and traditional criminals face, especially the tradeoff between efficiency and security (for example [113][114][115][116][117][118][119][120][121]). Protective controls are recognized by these scholars as being vital to criminals and terrorists to evade counter-attacks by fellow criminals and/or avoid detection and arrest by law-enforcement agencies. Yet deviant security itself is not an object of study. Security of traditional criminals seems to be a given in these papers; as something that is understood to be really obvious which does not require any further explanation.

3.1 Computer Science & Engineering Literature

This section presents four representative examples of technical research that discuss aspects of deviant usage of security by cyber criminals: i) anti-forensics, ii) botnet protection, iii) authorship analysis and iv) attacker economics. Many of the reviewed studies on the first three themes are exploratory or descriptive in nature. They shed light on *how* cyber criminals apply - i.e., practice - deviant security. These reviews present what each theme is about, how the literature fills in the various components of the security cycle, what the methodological strengths and weaknesses are in some approaches, and implications for this study. Because these themes are not explanatory in nature, a fourth theme is added to this review. Research on attacker economics implies a new subdiscipline - the economics of deviant security - which adds explanatory power to this study as to *why* cyber criminals make certain deviant security-related decisions.

3.1.1 Anti-Forensics

Studies on anti-forensics are limited compared to the total body of research on digital forensic research [122]. In this section, papers have been reviewed that are labelled as anti-forensics or use anti-forensics in their list of key words or text. Confusingly, in much of the literature the referent object is ambiguous: it is either a private investigator who are confronted with anti-forensics (AF), or an undefined security recipient who is threatened by digital forensics and therefore in need of anti-forensics (see Figure 3.1). As a result, many components of the security cycle are unclear or even unknown.

What is research on anti-forensics about? In the past, digital forensics was relatively easy and even named the 'Golden Age of Digital Forensics' because of - amongst others - little encryption and storage, and few file formats and operating systems [123, p.66]. Digital forensics have become much harder due to technologies that deny investigators to access case data. The long and rather broad list of techniques and tools that thwart investigators, forensic tools and investigations are collectively called anti-forensics or counter-forensics [124][125][126][127][128][129][130][131][132]. These anti-forensics attempt to compromise the confidentiality, integrity and availability - thus usefulness - of evidence in the forensics process [133, p.45][134, pp. 67-69]. In this sense, most of these studies are multidisciplinary in nature as they link computer scientific challenges to the legal world in which digital forensic researchers and investigators operate. Proposed taxonomies include categories as data hiding (e.g., encryption, steganography), artefact wiping (disk-, log-, and metadata wiping), trail obfuscation (data fabrication, IP-spoofing), analysis prevention (anti-reverse engineering, program packers), and techniques that complicate and/or delay digital forensics (data pooling, dummy hard disk drives) [135][134][132].

Security cycle on anti-forensics How should these counter-forensics be understood in terms of security? Let us take child sexual abuse material as an example as there are many papers that analyze anti-forensic techniques which target visual information (such as [136][137][138]). Using the security language from Section 2.1, we would expect that literature about anti-forensics sees police investigators as threat agents whom attack the computing systems of computer-assisted CSAM users with digital forensic tools. To avoid an instance of being exposed to losses on their computing system, such as a valuable CSAM collection, anti-forensics are deployed to mitigate the potential risk that the abuse images are destroyed or become incriminating evidence against the CSAM user (see court cases like [139]). That is, however, not the scope of much of the literature on anti-forensics.

Not criminal-centric... The current perspective in anti-forensics is not criminal-centric (thus taking cyber criminals as referent objects) but digital forensic-centric in the sense that digital forensic tools tend to be point of focus. However, approaching anti-forensics from the viewpoint of the cyber criminal reveals several gaps in our knowledge about anti-forensics. Counter-forensics are indeed in themselves neutral security mechanisms, used by individuals and organizations with either good or bad intentions [125][140, p.137]. Although scholars have stressed that AF like secure-deletion must be evaluated with respect to the adversary [141], most studies - with exceptions like [142] - do not place counter-forensics within a larger deviant security context. They give little information about the:

– deviant security policies on which these mechanisms are based;

- malicious referent objects who deploy anti-forensics (computer-assisted criminals, computer-focused criminals, or also traditional criminals?);
- threat agents that attack anti-forensics (only bonafide investigators or also other criminals?);
- vulnerabilities that these counter-forensics have to control, and the assets they have to protect.

These papers thus imply that the situations in which anti-forensics are deployed do not differ between cyber criminals and law-abiding entities. Timestamp modification, however, is solely focused on affecting the integrity of data to prevent information from becoming evidence in court, and/or even provide *ex culpa* evidence. It is not an effective technique for legitimate enterprises to defend themselves against criminal attackers without damaging their own daily business proceedings.

...and not police investigator-centric Anti-forensics do not rely on a single countermeasure, but on a large collection of constantly evolving techniques to defeat computer forensics [124, p.21]. However, studies about anti-forensics generally do not describe the coherence between various counter-forensics, nor the interplay with the deviant security mechanisms that are thwarting the investigative steps prior to, and after, the deployment of digital forensic tools (see [143] for an overview of the different phases of the digital investigative process). For example, a CSAM offender used the anonymous communication network Tor (also known as The Onion Router), regularly changed nicknames, and installed a virtual machine (VM) on his laptop for the sole purpose of storing encrypted abusive content, but completely deleted the VM, wiped his hard disk and cleaned his house after a co-conspirer was arrested by law-enforcement [144]. This example illustrates that threat agents of cyber criminals encounter more deviant controls than just attacks on their tools during their investigations. However, these issues are not addressed since mandated breachers of deviant security are not the audience of most anti-forensics studies. So, although it has been suggested that anti-forensics are an indicator of malicious intent (i.e., a prime goal for police investigators to establish) [145], the reviewed papers are also not police investigator-centric (thus taking police investigators as referent objects) [146]. The focus is very much on AF that private investigators discover, namely anti-forensics against data at rest encountered in an offline environment or private network which is subsequently examined in digital forensic laboratories [20, p.207]. Studies that provide empirical evidence for anti-forensics against data in motion and in Internet environments and related vulnerabilities and exploits - such as preservation or interception of data which is the exclusive terrain of public law-enforcement agencies - are scarce, with notable exceptions like [147].

Little attention for vulnerabilities in anti-forensics Moreover, the digital forensic-centric approach holds in essence a negative perspective. Anti-forensics indeed exploit vulnerabilities in the security of the digital forensic process. This viewpoint, however, puts investigators and forensic examinators always on the defense. It ignores that security controls, including anti-forensics, have vulnerabilities as well. This negative perspective in the literature might be the reason that exploits in AF - known as anti-anti-forensics [148], and counter anti-forensics [142] - are sparsely explored [145].

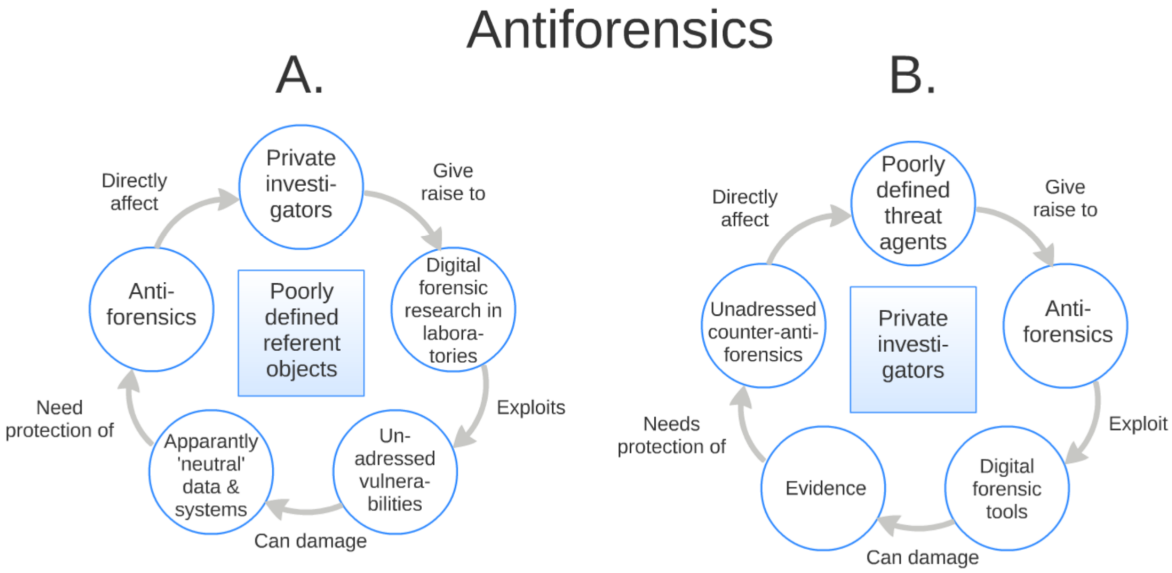


Figure 3.1: The referent object in AF literature is ambiguous. Irrespective whether referent object A. or B. is adopted, many components of the security cycle remain unclear.

3.1.2 Botnet Protection

Compared to literature on anti-forensics, studies about botnet protection are able to fill in most components of the security cycle. Yet these studies have a narrow focus, and therefore miss out on alternative threat agents of, and attacks on, botnets and subsequent deviant countermeasures by botnet herders (see Figure 3.2).

What is research on botnet protection about? Another field of study that discusses aspects of deviant security, but which is written from a more criminal-centric perspective, is applied research about botnet detection and monitoring. Botnets consist of infected computers under control of a botnet herder, and are named as the preferred tool for cyber criminals, because of - amongst others - their ‘nearly impenetrable shield of anonymity for [the botnet herders] themselves' [149]. Scholars have addressed various protective measures of botnets that hinder detection, sometimes even exploiting vulnerabilities in botnets [150], and formulated countermeasures against botnet infrastructures. These papers mention 'defensive skills' of botnets (e.g., command authentication, encryption and obfuscation) [151][152][153][154][155]; 'botnet enhancing techniques' such as 'resiliency' and 'stealth' [156][157]; 'anti-recon[naissance] techniques' namely deterrence, passive attacks (i.e., black-listing), active disinformation and retaliation attacks [158]; and vulnerabilities in botnet infrastructures while referring to technical computer security concepts such as the CIA triad [159][160][153][155]. In general, these studies combine the formulation of high abstraction deviant security policies categories with empirical evidence that these policies are implemented by countermeasures.

Security cycle on botnet protection These botnet studies have a well-defined referent object in mind: the botnet operator (also called the bot herder). The following line of reasoning is found in most botnet studies. The tools to commit cyber crime are assets to the herder. In this case, the malicious software and botnet architecture including infected systems and command-and-control (C&C) servers represents a financial value. The operator either invested time and efforts to develop the botnet him/herself or bought components on the cyber crime-as-a-service economy like infected hosts. To protect the availability of the botnet against takedown by threat agents, the botnet operator opts for security policies based on e.g., resiliency and business recovery which are - amongst others - enforced by hosting not one, but several C&C servers. Because referent objects are clearly defined, the focus and scope of botnet studies is more security-oriented than AF studies. Still, the way that botnet studies fill in components of the security cycle reveals several research gaps that are discussed in the next two paragraphs.

Beyond botnet disruption Because these studies have a strong focus on botnet activity (as compared to the individual, i.e., the botnet operator), many papers focus on disruptive interventions. The threat agents that have to execute these attacks - i.e, botnet infiltration, sinkholing or infection notifications [161] - are cross-sectoral public-private consortia [162], to the extent that universities participate in takedowns [158]. Some multidisciplinary studies also take legal practitioners as their the audience, and explain how proposed attacks against botnets translate to investigative powers. Despite the crucial role of the private sector in botnet takedowns [163], only law-enforcement agencies (LEA) have the legal mandate to exploit the vulnerabilities of botnets and ability to overcome cross-jurisdictional challenges. Moreover, few studies consider offensive exploitation of C&C vulnerabilities [155], while attribution of the botnet herder - another exclusive domain of LEA - is often not considered at all. Ultimately, botnet activities will only stop when the operator is identified, arrested and successfully prosecuted. As the first botnet takedown analyses - very much outcome evaluations - show that takedowns are not always effective [164][165][166], process evaluations - how takedowns were executed - are still absent. Similarly, there is little attention for infected machines of victims - known as bots - which are an important asset of any botnet and therefore in need of deviant security. While sinkholing botnets is helpful to redirect infected machines away from the botnet herder, studies on follow-up issues are absent such as about the identification, differentiation and notification of victims. There is a need for evidence-based methods and techniques that filter out false positives and identification high-value botnet victims.

Botnets as offensive countermeasures With the exception of [158], botnet studies generally focus on the defensive capabilities of the botnet infrastructure without exploring botnets as offensive countermeasures. Yet the list of botnet attacks for protective purposes is long. There are reports about DDoS attacks against banking fraud victims to hinder investigation [167], against websites of investigative journalists who report about botnets and their herders [**?**], or against competing online pharmaceutical affiliate programs [168, p.3]. These reports of botnets as tools for offensive countermeasures provide another argument that deviant security practices may differ from law-abiding security practices. Determining whether a botnet attack is launched as a pre-activity for the commission of crime - i.e., a stepping stone - or as a post-activity for the protection of crime is important to the cyber security community.

A last observation about research on botnet protection is the strong focus on security failures of botnets, rather than successful instances of deviant security. What are successful re-occurring security features of botnets on a high level of abstraction, and are they consistent through time? Moreover, are the majority of botnet vulnerabilities caused by accidents, failures and mistakes, or by increasing capabilities of the cyber security community in a larger cat and mouse crime game?

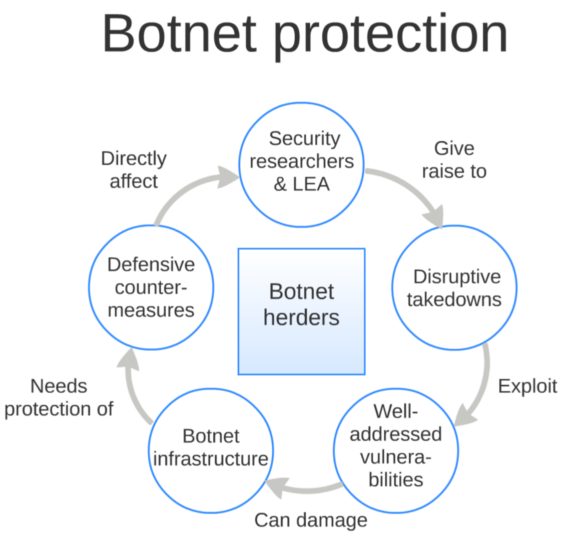


Figure 3.2: While most components can be filled in by the literature on botnet protection, the scope of these studies could be broader. There is, for example, little focus on botnets as offensive countermeasures and alternative interventions against botnets.

3.1.3 Authorship Analysis

Compared to the two previously reviewed themes, studies on authorship analysis have the most broad and rich deviant security approach, and hold several methodological lessons for this study (see Figure 3.3).

What is research on authorship analysis about? A third theme in computer science that evolves around deviant security is authorship analysis (also called stylometry), which relies on machine learning, statistical analysis and text mining techniques for criminal identity tracing. Authorship analysis has, for instance, been applied for attribution purposes on online communications [169][170][171], malware code [172][173][174], and phishing websites [175]. Not only does authorship analysis serve attribution in police investigations. Stylometrics are even considered evidence in courts around the world [176].

Security cycle on authorship analysis This field of study fills in the deviant security components as follows. All hardware, software and data that lead to the criminal's true, offline identity are important assets that are in need of security. Written texts - such as the presence on a cyber criminal forum, usage of chat services, development of malware code - are necessary to commit crime. To avoid attribution, cyber criminals apply - amongst others - security policies on a metadata level, like deception (e.g., usage of multiple online monikers). They might also try to withhold personal details during communications from other criminals on a content level. However, written texts - whether data or software

- work as a unique fingerprint of its author, and reveal much about gender, age, ethnicity, occupation, intelligence, skills, and, ultimately, offline identities. Therefore, criminals might deploy additional security against authorship analysis (also known as adversarial stylometry) such as obfuscation, imitation and machine translation to control this vulnerability [176]. While hardware configuration might be subjected to authorship analysis [177], deviant countermeasures against it have yet to be discovered.

The need for empirical data & perspectives of research participants Framing authorship analysis in a wider deviant security perspective reveals important insights for this research project. For example, circumventing authorship recognition is a deviant security policy that does not ensure but *affect* the integrity of data. In such a situation, criminals essentially decrease the assurance of the accuracy and reliability that texts are written by them. This significantly differs from security policies that are prescribed by industry standards. Although we know about the existence of legitimate software to evade authorship analysis, ground truth data of cyber criminals actually deploying these techniques is absent in the reviewed academic literature. Research on malware code re-usage in the cyber criminal underground is still in its infancy [178], and how to detect and distinguish multiple individuals working on the same malware is still unknown. Moreover, information from police investigations shows us that cyber criminals, besides machine translation, deploy human translators to write texts for phishing websites or advertisements on cyber criminal fora [179, pp.31-32]. This practice increases the accuracy of the grammar in texts and thus the conversion rate of attacks, but also holds defensive qualities, especially from the viewpoint of those who investigate these crimes: authorship analysis would not point to the suspect but to e.g., an ignorant, but bonafide translator. So, the conceptualization of DevSec is not only shaped by those who apply security, but also by those who are confronted by it.

Multidisciplinary approach & new academic disciplines The strength of authorship analysis research is its multidisciplinary approach between computer science and linguistics, testing of tools, mixed criminal and investigator-centric perspective, and focus on the criminal individual and his/her conduct. While some have briefly addressed the importance of cultural dimensions in authorship analysis research that will benefit police investigations [169], much of the research evolves around computer-mediated *English* instead of computer-mediated *communication* [180, pp.4-5]. This touches upon explanatory theories for deviant security. The anthropology of deviant security (research on e.g., how security culture changes over time and space) and the linguistics of deviant security (research on e.g., the form and meaning of cyber criminal language usage) might well be new academic disciplines to study these dimensions. Cyber criminals communicate via short chat and forum messages, sometimes exclusively in Cyrillic alphabet, and/or contain specific hacker argot to keep rookies and law-enforcement out. Would authorship analysis also work on short conversations in

Russian, littered with argot? Such insights into the (inter)cultural dimensions of cyber crime in general, and deviant security specifically, contribute to effective police investigations. Text in the English language written by non-English speakers, or in dialect, might reveal the criminal's country or region of origin, and subsequently help LEA to identify potential subjects of interest and prioritize cases. There are other unexplored disciplines that will explain DevSec practices and improve police investigations, the economics of deviant security being one of them. The next section explains this discipline in more detail.

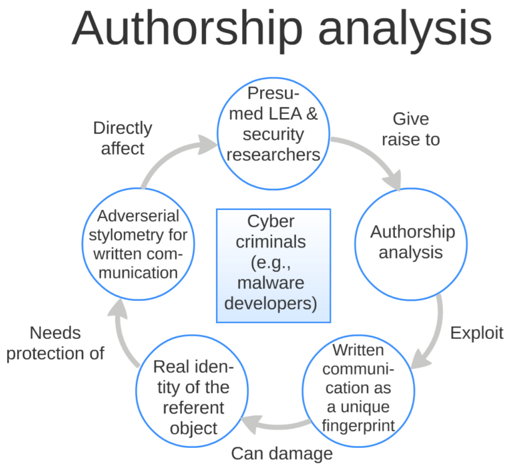

Authorship analysis
Presumed LEA & security researchers
Give raise to
Authorship analysis
Exploit
Written communication as a unique fingerprint
Can damage
Real identity of the referent object
Needs protection of
Adverserial stylometry for written communication
Directly affect
Cyber criminals (e.g., malware developers)

Figure 3.3: The multidisciplinary literature on authorship analysis has a broad scope and is rich in insights on DevSec. Moreover, these studies also hold various methodological lessons for this study.

3.1.4 Attacker Economics

The literature of the last theme - attacker economics - is not of a descriptive, but of a more explanatory nature. Attacker economics studies currently have law-abiding referent objects as a focal point who are under attack by malafide threat agents. Just like the previous themes, this section begins with explaining what the topic is about, but then proceeds with presenting an important sub-theme within attacker economics for this study: the economics of deviant security that focuses on the cost-benefit analyses of cyber criminal referent objects about their technical computer security practices.

What is research on attacker economics about? Economics of information security is a synthesis between computer and social science, and combines microeconomic theory, and to a lesser extent game theory, with information security to gain an in-depth understanding of the tradeoffs and misaligned incentives in the design and deployment of technical computer security policies and mechanisms [181, p.610][182, p.358]. Most papers within this discipline are written from the good guy perspective on security. For example, Van Eeten and Bauer studied the incentives of legitimate market players - such as internet service providers (ISPs) and software vendors - when confronted with malware [183]. Papers that are written from the bad guy perspective - so called attacker economics - are gaining importance as well (for example, [184][185][150]). Attacker economics exposes cost-benefit analyses of attackers to exploit vulnerabilities in the security of the victim target, to subsequently formulate protective countermeasures for law-abiding entities [186, p.3]. The strength of these socio-technical papers is their acknowledgement that security is very much a human problem, and the combination of behavioral science with technical computer security is currently one of the most thriving and fast-moving disciplines to increase our understanding of the law-abiding entities' and cyber criminals' decisions to respectively secure their systems or optimize attacks [181, p.610]. The identified cost-benefit analyses in these papers are not related to deviant security, but to the offensive side of committing cyber crime, namely the attack itself such as [168].

Economics of deviant security Several of these attacker economics papers imply that there are also economics of deviant security. Herley, for example, has written about the fundamental tradeoff that Nigerian spammers must make between the gain from true positives and the cost of false positives [187, p.13]. He proposes to add false positives to reduce the attacker's return, and mentions scam-baiter sites whose visitors intentionally lure Nigerian scammers into time-wasting conversations. The unnoticed link to deviant security lies in the fact that scam baiters breach the security of spammers by social engineering their criminal 'victims'. Basically, scam baiters try to exploit the spammers' vulnerability of being greedy, see Figure 3.4. Another example is Herley and Florencio's study about the low tier underground economy on IRC channels that are 'occupied by those without skills or alliances, newcomers, and those who seek to cheat them' [186, p.1]. This suggests that the cyber criminals who operate in this market have to protect their valuables against other cyber criminals such as rippers. Although these papers have been criticized for lacking empirical data, and applying an economic meta-analysis to make their case [188, p.2], they prove an important point. Attacker economics currently tends to focus on the commission of cyber crime to formulate protective responses for (the computing systems and information of) law-abiding referent objects. However, attackers are also in need of security which previous papers have overlooked. Attacker economics should therefore also encompass the economics of deviant security that focuses on the tradeoffs related to the protection of cyber crime and offensive responses of law-enforcement agencies.

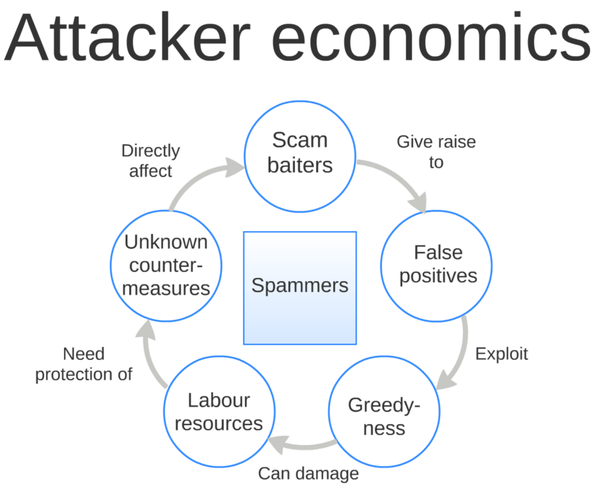


Figure 3.4: While attacker economics generally takes law-abiding entities as referent objects of security, Herley's paper on scam baiters fits within the deviant security process cycle [187]. The cycle reveals that effective deviant countermeasures against scam baiters are largely unknown to academics.

3.1.5 Interim Conclusion & Discussion

This section reviews deviant security related themes within computer science and engineering to understand *how* cyber criminals apply protection, to conclude that there are many open questions that touch upon the what, who, where/when, and why of deviant security. In other words: methods and techniques of DevSec are revealed by researching the basic empirical and normative qualities, key players and interactive qualities, temporal-spatial qualities and rational (cost-benefit) motives of deviant security. For example, the rigorous and in-depth research on the protection of botnets raises numerous question marks about the deviant security practices of other cyber crimes. *Who* else applies deviant controls? There is considerable literature on botnets because they are most apparent to researchers. Botnet herders are end-users of the underground economy in the most visible part of the value chain. They make victims by committing bank fraud or sending spam; their crimes and infrastructure thus become noticeable to researchers and legal practitioners. The same argument holds for anti-forensics that are encountered as soon as data that might hold evidence is preserved by investigators. What about less visible cyber criminals and deviant security practices? Academic research on bulletproof hosters, their activities and infrastructure is virtually absent, although the core business of these malicious hosters is essentially deviant security. These *who* questions touch upon the idea of conducting comparative research: do computer-assisted criminals differ from computer-focused criminals in their security? The existence of bulletproof hosters, who basically sell security as a commodity, raises questions about *what* the basic normative and empirical qualities of deviant security are, i.e., its distinctive characteristics, incorporating both the perspectives of both those who apply DevSec as those who are confronted with it. Because many protective technologies on their own are neutral and serve a dual-use purpose (see also 3.3), the security policies on which they are based are affected by specific situations (i.e., time and space), and therefore point to questions about *when* and *where* deviant security is applied. Lastly, insights from the previous questions may also shed light on *why* criminals apply DevSec, i.e., their short and long term motives. Although the identified security policies and security mechanisms of cyber criminals are largely technical computer security, computer science alone cannot provide answers to the above questions. Synthesizing insights from technical computer security with social science and legal scholarship helps to gain a comprehensive understanding of deviant security as the next sections show.

3.2 Social Science Literature

Previous sections show that computer science cannot provide answers to many deviant security-related questions, and pays less attention in understanding the behavior of those who try to breach technical computer security and subsequently placing their actions within criminal law. On the other hand, the multidisciplinary discipline of attacker economics proves there is much to learn from social sciences. More specifically, social science helps to formulate a new definition for modus operandi that emphasizes the need for suspects to protect the criminal and his/her crimes.

A new definition for modus operandi Much research in social science is undertaken to understand the actions that a cyber criminal has to take to perpetrate a crime. These actions are called *modus operandi* or method of operation (MO) by academics and legal practitioners [189, p.24][190, p.89], and tactics, techniques and procedures (TTP) by the private security industry. An MO generally relates to *how* a crime is committed, and serves the ‘successful completion of the crime’, ‘the protection of the offender’s identity’ and ‘the facilitation of the offender’s escape’ [191, pp.287-288]. These purposes let us realize that an MO is actually also very much about deviant security. Yet most social science studies about cyber offenders put an emphasis on understanding the commission of crime, ranging from the online grooming of children and/or collection of child abusive material by sexually-driven computer-assisted criminals [192][193][194], to the networks, organizations and platforms of financially-driven computer-focused criminals [195][196][197].

The commission *and* protection of cyber crime are, however, inextricably linked to such an extent that is hard to find instances where there is absolutely no security prior, during or after the commission of cyber crime. Crime without deviant security implies the use of non-obfuscated malware, real credentials to register domains for botnets, a suspect’s home Internet protocol (IP) address to connect to victims, a suspect's bank account to receive stolen money, non-encrypted hard drives, and open conversations about malicious activities to strangers. Of course, these situations rarely happen, let alone all together. Data, systems and communications become valuable - and thus are in need of protection - because they relate to either the:

- *Criminal*: everything related to the suspect's online and offline identity and his/her physical and mental integrity; and/or
- *Crime*: the collection of related, structured activities designed to produce a specific product, service, or other cyber criminal output [198, p.210].

Therefore, this study defines modus operandi as:

> *The commission of crime, and the protection of crime and the criminal.*

Nota bene, all commission and protection practices fall within this definition, forming a continuum that ranges from a preparation and pre-activity phase to an activity and post-activity phase [199]. Furthermore, the emphasis on the criminal and (the outcomes of) his/her conduct are two core dimensions of the study of crime (the other two being enforcement and victims [20, p.3]), and dovetails with the notion of *who* and *what* attribution in criminal proceedings. Because of this link to the world of legal practitioners, the definition - including the distinction between commission and protection - is an essential feature in this study. While there is excellent social science research on the commission of cyber crime (e.g., [200][201][34]), the emphasis of this study is obviously on the latter part of the definition. Therefore, the next sections briefly explore what social scientists write about the protection of cyber criminal's identity and his/her malicious business proceedings, and conclude that a technical computer security perspective adds to a better social science understanding of deviant security.

The protection of the criminal When describing and explaining cyber crime, social scientists mention the nature of the Internet ([50, p.44][89, p.6]) and the deployment of privacy-enhancing technologies (PETs) [28, pp.140-141, 148] - like encryption - that protect the cyber criminal's identity [202]. The resulting anonymity ([203][169, pp.59-60][204, p.7][205, p.75]), enables offending [203], and helps to evade detection and prosecution [28, pp.140-141]. It is for good reason that the United States Department of Justice names anonymity the greatest asset of cyber criminals [206].

How should these aspects of the protection of the cyber criminal be understood in terms of security? Using the components of the synthesized security analysis, cyber criminals seem to regard their online/offline identity and physical/mental integrity as valuables. However, the use of certain information technologies - such as an IP address of a home network router - makes the cyber criminal vulnerable to attacks by law-enforcement agencies whom may request information for identification purposes from third parties, like ISPs. So, cyber criminals deploy countermeasures, such as the use of a VPN [112], to protect their true offline identity, and as a result remain anonymous. This security analysis is a simplification, but nevertheless reveals several research gaps. For example, the reviewed social science studies do not link anonymity to technical computer security concepts. Anonymity is an important factor of confidentiality [36, p.10], and about the ability to communicate without revealing identity [64, p.44]. From an attacker's perspective, anonymity is about not sufficiently being able to identify the subject within a set of subjects [207, pp.9-12]. By linking anonymity of identity to the CIA triad, it becomes apparent that deviant countermeasures have to protect more than the online and offline identity of the cyber criminal; it raises the question how factors within the other two concepts of the security triad - integrity and availability - relate to security for cyber criminals. For example, how do cyber criminals protect the availability of computing systems against DDoS attacks from other cyber criminals?

The protection of crime Crime implies behavior performed by a criminal, or in legal terms, a suspect [80][208, pp.71-72]. Throughout this study, different terms - criminal business proceedings, illegal output of malicious behavior, and so on - are used to point out that the protection of crime also implies conduct. Although there is much written in social science about the protection of the cyber criminal's identity, few studies explicitly discuss the protective measures of suspects whom commit cyber crime. Newman and Clarke mention several 'criminogenic attributes of the computing environment' that relate to security policies of cyber criminals protecting their business operations:

- *Stealth* ensures that crimes are invisible;
- *Challenge* that cyber criminals will take as little time necessary to carry out the criminal act, decreasing the chance of being caught;
- *Escape* that 'there is little sense in planning and carrying out a crime if it is obvious that the chances of getting caught at the time of the act are very high, or that a trail of evidence is left that will lead inevitably to detection' [209, pp.61-63].

Turvey further lists examples of MO behaviors related to deviant security such as offense location selection (i.e., 'a server hosting illicit materials for covert distribution'), and offender precautionary acts ('the use of aliases', and 'IP spoofing'). He concludes that successful cyber criminals are those who avoid both detection of their crimes and identification [191, pp.288, 292].

Again, technical computer security helps to structure the specific security mechanisms behind these abstract security policies. Technical computer security also helps us to understand that data, systems and communications become assets, not only when they are related to the criminal but also to crime. Stealth is achieved, according to Newman and Clarke, by 'remote storage on an innocent third party's computer' [209, p.61]. Firstly, stealth is defined in the Oxford

English Dictionary as ‘cautious and surreptitious action or movement’ [210]. We therefore link stealth to criminal actions - read: crimes - as compared to the criminal. We further connect stealth to the security goal of *unobservability* which is, in turn, an attribute of *confidentiality* [64, p.44], and about *undetectability* of items of interests against all subjects [207], such as the undetectability of child abusive material against the threat agent of LEA. Secondly, remote storage on a third’s party computer points to an online form of dead drops: an operational security technique to exchange information without being connected directly to another individual. CSAM offenders frequently exchange their abusive material by uploading encrypted images to a file share service, and subsequently post the hyperlink of this third party website and/or related password on an access controlled forum so others can access and decrypt the material. Using a cryptocurrency tumbler, affiliate partner programs [211], or unwitting moneymules as intermediaries to launder dirty money is essentially a comparable situation [212], just like usage of anonymous remailers to send messages [36, pp.443-445]. These are all instances of dead drops - i.e., proxies - that provide stealth, or in terms of technical computer security: unobservability and undetectability [207].

In all of these cases, security policies and mechanisms are installed to protect data (e.g., child abuse material), systems (botnets) and communications (peer-to-peer file sharing) - assets related to either the identity of the criminal and/or his/her malicious activities. The opposite may also occur. Data, software and systems do not necessarily hold importance to the criminal. Research suggests that compromised Web servers for conducting spam runs are not protected by the criminal, because spamming hosts do not require to be accessible to victims, as compared to phishing hosts [213, pp.176-177]. In other words, systems used for spam do not hold any value for the criminal after the crime is committed.

A last observation is the absence of empirical data in social science studies about DevSec which holds lessons for the methodological direction of this study. Although it is easy to imagine that, for example, escape is vital for the successful commission of cyber crime, both Turvey, Newman and Clarke give little empirical evidence for their claims, which is understandable as cyber crime studies in general lack theoretical and empirical evidence [28][34][80, pp.86-89]. Nevertheless, these social science papers demonstrate that the same security policies might be found across disciplines on a high level of abstraction (such as stealth which is also found in computer science papers on botnet protection). Moreover, these papers stress the importance of using data collected in the field, and of applying a ‘human-centered’ and ‘human factor’ approach to increase our understanding of the behavior of cyber criminals to develop better means of discouraging and disrupting their crimes [214][215].

3.3 Legal Studies

We derive from social science that the commission of crime and protection of crime and the criminal are inextricably linked. Crime can not be successfully committed if a criminal does not take any necessary precautions against other criminals or law-enforcement agencies before, during and after their malafide conduct. Criminal law follows this dichotomy between commission and protection. Simply put, substantive law focuses on the commission of crime as it defines crimes and establishes punishments [82, pp.7-13]. Generally, if a crime is committed and identified as such, procedural law begins. Hence, criminals apply security to avoid encounters with the threat agent of law-enforcement agencies and related attacks of investigation and prosecution. This raises the question how procedural law deals with instances of deviant security. This section explains why investigative powers are a *means* to exploit vulnerabilities in the security of cyber criminals, thus affect the criminal's CIA triad, to gather evidence while simultaneously hold an additional *objective* beyond the goals currently acknowledged by legal scholars and legislators. The mere threat of investigations disrupts the cyber criminal process.

Means: legitimate attacks on deviant security There is a so far unnoticed relation between on the one hand deviant security that protects crime, and on the other hand procedural law which governs the investigation and prosecution of cyber crimes. Many procedural laws (and thus police investigative powers) not only aim at breaching the security of criminals in order to identify the suspect and obtain evidence related to his/her criminal activities, but also affect the confidentiality, integrity and availability of deviant security. So criminal procedure not only protects the rights of the suspect and others involved in an investigation by regulating the power of the police [20, p.397][82, pp.13-18]. The law further prescribes how and when the police is allowed to exploit both technical and human weaknesses in MOs to gather evidence. This argument very much makes law-enforcement mandated breachers of MOs in general and deviant security specifically. The components of the synthesized security analysis shed light on the relation between the protection of criminals and investigative powers of law-enforcement agencies. As an example, mandatory password disclosure - implemented in the United Kingdom and once proposed in the Netherlands - is a coercive investigative technique to deal with encryption applied for illegal purposes. A suspect may have an information asset - for example, child sexual abusive material - that he protects in an encrypted container. Law-enforcement will try to exploit the suspect's vulnerability of fear for incarceration by threatening with a prison sentence if the suspect does not hand over his/her password. Another example is the legal proposals in the United States of America and the Netherlands for the allowance of police hacking [216][217]. Cyber criminals may protect their valuable online market place with access control management. A successful brute force password attack by LEA exploits the vulnerability of a weak password to access a legitimately seized criminal forum. These, and other examples [218], show that investigative techniques are closely related to the CIA triad. Access control and encryption both preserve the confidentiality of a security system [54], and mandatory key disclosure intends to affect that confidentiality. A coordinated takedown of a CSAM site by ISPs and law-enforcement agencies affects the availability of the illegal content.

Investigative powers further follow the same underlying principles of cyber criminal TTPs that exploit vulnerabilities in the security systems of their victims, including human weaknesses. Cyber criminals apply social engineering - the art of intrusion and deception [219][220], with or without the use of technology [221] - to convince (potential) victims to disclose confidential data or perform another action [222]. Covert investigative techniques (also known as undercover powers), such as infiltration and pseudo purchase/services, exploit human vulnerabilities and are basically social engineering applied by LEA.

These examples show that the technical computer security understanding of attacks (see [54]) helps to conceptualize investigative powers in cyberspace. Wiretaps are obviously *interception* attacks, while takedowns are *interruption* attacks, and undercover powers are *fabrication* attacks. The criticism of legal scholars and computer scientists on police hacking - such as the argument that law-enforcement officers can alter evidential data - is basically about the possibility that this investigative power becomes a *modification* attack which is not compatible with the legal principle of evidence integrity. The finding that investigative powers aim at breaching the security of cyber criminals leads to another conclusion; it implies that comprehensive policies within the border-centric view on cyber security and cyber crime that include police investigations also encompasses an understanding of deviant security.

(Additional) objective: disruption of modi operandi According to legal scholars and legislators, criminal law with well-defined punishments has a number of objectives. It aims at - amongst others - incapacitation, general- and specific deterrence and rehabilitation [223, pp.889-922]. These objectives are very much focused on preventing future crimes, and as such, criminal law intends to have real world effects on how citizens behave in society [224, pp.79-84]. However, when criminals do commit crime, merely restrictive deterrence - limiting the frequency, magnitude or seriousness of offenses - is left as an objective of criminal law [225, pp.35-36]. Does criminal law has any other effects on the criminal who is already busy with committing crime? Indeed, it is - amongst others - *because* of criminal law that cyber criminals are forced to protect crimes and their identities. This implies that criminal law has effects beyond deterrence that are directly related to deviant security. Although it has been argued that the state's capacity to deter criminals from committing cyber crime might be limited [226], the ever-present threat of law-enforcement has a real-world effect on those that are not deterred by criminal law. So, an additional objective and consequence of procedural law and police investigations can be understood in terms of the economics of deviant security. The threats/attacks by LEA force cyber criminals to apply security and as such, negatively affect the commission of cyber crime. In other words, the mere existence of these legal tools increase the costs of cyber crime as suspects have to invest (e.g., time, money) or turn down (reject a potential business partner) resources into/for their security, and as such, decrease the efficiency of malicious business operations. Criminal law, both as threat and attack, is therefore essentially *disruptive* to the cyber criminal business process. Legal practitioners suggest that law-enforcement agencies will no longer have the resources to investigate or prosecute all cyber crime, and should shift towards disruption of the cyber criminal process [227] while academics from predominantly computer science have already been discussing the technical possibilities of such disruptive interventions [185]. Yet legal studies about criminal procedure in cyberspace heavily focus on attribution of offenders rather than researching the opportunities and legal feasibility of applying investigative powers for disruptive purposes.

3.4 Interim Conclusion and Discussion

Although Section 2.2 concludes that current security discourses evolve around good guys who protect themselves against attacks by bad guys, academics and experts do touch upon aspects of deviant security of cyber criminals. The insights from computer and social sciences, including economics of information security, suggest that cyber criminals face more threat agents and threats/attacks than just law-enforcement agencies conducting police investigations. Subsequently, it is likely that related vulnerabilities, risks, valuables and countermeasures are different as well. For instance, online identifiers are indeed important data assets for cyber criminals, but financial assets also need protection because other criminals will try to steal them. Therefore, suspects of cyber crime not only apply anti-forensics to thwart digital forensic tools, but also deploy other, largely unknown, security policies and mechanisms that may differ from law-abiding entities who do not have to evade LEA. Legal scholarship contributes by revealing that criminal procedure subsequently intends to exploit the vulnerabilities in this security system. We now understand how these three academic disciplines - computer science and engineering, law and social science - help to describe and explain DevSec.

Bearing in mind three major methodological issues in researching cyber crime - the lack of: i) empirical data, ii) comparative and transnational research and iii) cyber crime research paradigms [50, pp.54-55][80, pp.86-89][81, pp.1-3] - the findings of the reviewed themes (i.e., anti-forensics, botnet protection, authorship analysis and attacker economics) help to further fine-tune the methodological directions to study deviant security practices. Some of the reviewed studies are, for example, merely written from a digital forensic technology perspective, and lack a human-centered, and more specifically, a criminal-centric approach. Although there is overlap in terminology among academic disciplines - e.g., security policies such as stealth and anonymity - there are too few studies, like [228], that are truly multidisciplinary in nature. They do not combine theoretical concepts and empirical findings, nor methods and techniques, from both social and computer science to understand the security systems of different cyber criminals. Nor do they link research outcomes to the legal practitioners' world of procedural and substantive law and police investigations.

Because a theoretical framework on deviant security practices is absent, the research part of this study - i.e., part III - are grounded in empirical data derived from, and incorporating the views of, both actors of the social interplay, namely those who apply deviant security as well those who are confronted by deviant security. Although the sum of the reviewed studies does not represent a comprehensive overview of research related to deviant security, it nevertheless shows that academic and non-academic literature is in itself a data source that contributes to an understanding and conceptualization of deviant security practices. Collected and processed data about DevSec practices should be analyzed from multiple academic angles, especially linking computer science to legal scholarship and social science, and adding explanatory power by applying insights from economics of deviant security. In other words, social scientific methodology is needed to capture a social-technical interplay in which cyber criminals apply technical computer security in order to be safe from the legal actions of law-enforcement agencies. These first research steps on deviant security will contribute to the development of a broader, new field of study which goes beyond the practices of deviant security. It might, for example, also include the computer engineering of deviant security and psychology of deviant security that respectively focus on the system design - i.e., software and hardware, including technical vulnerabilities and associated exploits - of deviant technical computer security controls, and on the cyber criminal's individual thoughts, feelings, and beliefs about his/her security.

Part II

Methodology

Chapter 4

A Multidisciplinary Approach for Deviant Security

Researching cyber crime poses multiple methodological challenges. Many cyber crime studies use small and/or limited data sets of poor quality. Few studies have structurally and systematically examined the cyber criminal and cyber security community over long periods of time [229], and/or from a truly socio-technical-legal perspective. This study intends to overcome several of these methodological challenges. So far, the study has raised a problem experienced by academics and legal practitioners: the security practices of cyber criminals. How to research a practice that intends to affect the integrity, limit the availability, and increase the confidentiality of associated data sources? This study combines computer science and social science with legal scholarship, having permission of academic and government authorities to use confidential and unique data sets. The study aims at producing scientific research that is relevant for computer science and engineering, social and behavioral sciences and the development of law, investigations and policy, thus seeking and forming working relationships across disciplines [230]. The body of this study relies on social science methodologies of Grounded Theory and microeconomic theory to research the predominantly technical computer security - i.e., the administrative, physical and technical controls - of cyber criminals. As summarized in Table 4.1, the study ends with the discipline of law and economics to research investigative responses against DevSec relevant to especially legal practitioners.

Part	Chapter	Description with an emphasis on methodology	Methodology
	Chapter 1 - Introduction	The identification of one of the underlying problems of the current effectiveness crisis in investigations as experienced by legal practitioners: the security practices of cyber criminals.	
Part I - Literature Review	Chapter 2 - Current 'Good Guy' Perspectives on Security	A literature study on current good guy perspectives on technical computer and cyber security provides input for studying the new security paradigm of deviant security with law-breaking referent objects, and concludes that a deviant security practices should first be expressed in a qualitative matter as a full picture on deviant security is absent before more quantitative approaches can be conducted.	Literature study
	Chapter 3 - Touching upon Security Controls of Cyber Criminals	A literature study on four DevSec-related themes - anti-forensics, botnet protection, authorship analysis and attacker economics - shows that research on deviant security should be criminal-centric and multidisciplinary in nature, i.e., combine theoretical concepts and normative and empirical findings, methods and techniques from both computer and social science, and link research outcomes to the legal practitioners' world of criminal procedures and police investigations.	Literature study
Part II - Methodology	Chapter 4 - A Multidisciplinary Approach for Deviant Security	Outlay of the research design for this first in-depth study on deviant security practices and economics in the Information Age.	
Part III - Research Findings	Chapter 5 - What? - Basic Qualities of Deviant Security	The core categories of the technical computer security practices and economics of cyber criminals that stand out in secondary data sources about those who apply and those who are confronted with deviant security, and are considered the most relevant to legal practitioners.	Socio-technical research based on Grounded Theory, technical computer security principles and microeconomic theory
	Chapter 6 - Who? - Interactive Qualities of Deviant Security		
	Chapter 7 - When & Where? - Temporal-Spatial Qualities of Deviant Security		
	Chapter 8 - Investigative Responses Against Deviant Security	Suggestions for investigative approaches for legal practitioners to confront deviant security practices, based on the findings of the previous chapters and other normative and empirical findings.	Socio-technical-legal research based on Law & Economics
Part IV - Conclusions	Chapter 9 - The Outlook of Deviant Security	Reiteration of thesis objectives, a filled-in deviant security process cycle, summary of findings and future research directions.	

Table 4.1: This study is of a multidisciplinary nature. The research problem is derived from criminal procedure. Social science methods and techniques are applied to gain knowledge about the technical computer security practices of cyber criminals. The outcomes of this study aim at providing input for comprehensive policies, evidence-based law and effective investigations, thus very much at improving the work of legal practitioners.

4.1 Descriptive: Grounded Theory for Deviant Security Practices

Cyber criminals very much have security policies. They do not necessarily write down, explicitly dictate, or are even aware of the high abstract policies they apply. Still, these policies can be discovered by analyzing the underlying associated security mechanisms. Which qualitative inquiry fits best to construct a model on deviant security policies and mechanisms? For this study, the answer to this question is Grounded Theory (GT). This methodology derives theory from data analysis, instead of vice versa. Thus, GT does not focus on testing hypotheses taken from existing theoretical frameworks, but instead promotes the development of a theory of an action, process or interaction grounded in empirical data collected in the field [231, pp.2-6]. There are several versions of Grounded Theory, and this study uses elements derived from two approaches on GT.

ELS on cyber crime & preference for qualitative research The legal connotations of researching deviant security are evident. This study has very much a legal starting point as it identifies a problem that procedural law and police investigations face in confronting cyber crime: the security practices of cyber criminals. This study further has a legal end point, aimed at producing outcomes that will benefit public policy, criminal procedure and police investigations to affect the protection of cyber criminals. The methodology to achieve such an impact on legal practitioners is called empirical legal scholarship (ELS). Empirical legal scholarship is the research produced by the academic world to create better law, informed by reality instead of assumptions [232, p.910]. ELS is on the rise for years, with ever increasing numbers of studies, and academic studies on the discipline itself [232][233][234][235][236]. Current empirical legal studies on cyber crime are published in journals as the Cybersecurity, Data Privacy & eDiscovery Law & Policy eJournal and the Cyberspace Law eJournal; as reports that discuss - amongst others - CSAM and related laws, policies and investigations [85], or EU law and computer-focused attacks on the HTTPS value chain [237]; and/or as sources for civil law verdicts on e.g., intellectual property violations [238]. However, many of these studies do not label themselves as ELS, nor explain the discipline and/or used methodologies. Law itself lacks methodology to produce empirical results. Therefore, between the legal head and tail of empirical legal studies lies a body of research that relies on the scientific method of inquiry [234][230, p.866]. The word empirical in ELS points to the evidence about the world based on observation and experience, whether numerical (quantitative) or non-numerical (qualitative) [233, p.1]. Because deviant security practices have not been systematically and structurally researched as an object of study and because theory on deviant security is absent, qualitative inquiry is preferred over quantitative inquiry. Qualitative research is conducted when a problem needs exploration, when theory is absent, and when a complex, detailed understanding of an issue is necessary [239, pp.39-40][240, pp.12-15], also when such issues are related to law and policy [241][242]. Therefore, this study prefers qualitative over quantitative inquiry.

Traditional and constructionist Grounded Theory There are two popular approaches to Grounded Theory. The first approach is the *traditional* Grounded Theory, originally developed by Glaser and Strauss in 1967 and later modified by Strauss and Corbin [231][240]. The second and more recent *constructionist* approach to Grounded Theory was developed by Charmaz [243]. Basically, the two approaches differ in whether the researcher believes if theory is *discovered* as emerging from data separate from the researcher, or *constructed* from the data by the researcher. To complicate things further, there are also two views on traditional GT. After initially writing the methodology together, Glaser and Strauss developed different views on GT in time. Glaser's view is that an objective truth emerges from the data, and every researcher will discover that same picture when the GT method is properly applied [244]. Strauss, together with his co-author Corbin, stresses that a researcher has to actively obtain theory from data. They expect that each researcher will place the focus on different aspects of the collected data depending on their background, beliefs and values [240]. The second approach - constructivist Grounded Theory - argues that the researcher is part of the world and data that is studied. Multiple social realities exists, and past and present interactions with people, perspectives, and research practices influence the grounded theory. So, the constructivist approach is very much an 'interpretive portrayal of the studied world, not an exact picture of it' [243, p.10].

Another major debate in GT research evolves around the focus on either *social processes* or *individual experience* [245, p.76-78]. Glaser, Strauss and Corbin aim at localizing social processes in particular settings, which is about the interplay between relevant conditions, and the responses of the participants to those conditions and to the consequences of their actions [246, p.419]. Charmaz's focal point lies on individual experience which is more psychological in nature as it tries to capture the internal world of the participant. Despite these differences, both approaches acknowledge that scholars should specify 'those conditions and consequences, at every level of scale from the most "macro" to the "micro," and integrating them into the resulting theory' [247, p.274][243, pp.118-119]. This so called conditional and consequential matrix is a focal point of this study as explained in more detail in Section 4.2 and Figure 4.1.

A mixed approach in this study Glaser and Strauss stressed in their original work to use GT flexibly [231]. This study is no exception on this position as it makes use of elements of both the traditional view of Strauss and Corbin, and the constructionist view of Charmaz. The former approach dovetails with the legal connotations of this study. Data is collected selectively to develop a grounded theory on deviant security that is significant for legal practitioners in the public sector and serves the general public. Researchers with the same research questions but other beliefs and audiences might well find alternative deviant security concepts albeit using the same data. In line with Strauss and Corbin, this study further tries to catch the social processes of deviant security, thus its social context, causes and consequences, rather than the psychological aspects of deviant security for individual cyber criminals, such as their thoughts, feelings, and beliefs.

The constructionist version of Grounded Theory guides this research because of - again - the legal connotations of deviant security. The research population and their activities - cyber criminals and cyber crimes - are normatively laden concepts, and are therefore very much social constructions as well, rather than being objective and neutral 'truths' [40]. The security of cyber criminals cannot be 'discovered' when the implementation of such terms differs in time and across jurisdictions to the extent - as noted before - that law-enforcement agencies in authoritarian states without the rule of law conduct criminal behavior, as compared to the political dissidents such police units tend to investigate. The acknowledgement of the researcher that reality is a construct also touches upon the constructionist's emphasis on reflexivity. Going native in the cyber security community might be a positive type of research, as long as the researcher takes a reflective stance on the interpretations of him/herself and his/her research participants, and subsequently presents these to his/her audience [243, pp.130-131, 188-189][241, pp.9-10][248, pp.229-231].

4.1.1 Cyber Criminal and Cyber Security Participants

Criminals in general, and organized criminals specifically [249], are an unwilling population for research. They would rather not reveal their activities [250, pp.54-57]. (Organized) cyber crime is no exception to this rule, as there is a large dark number of undetected cyber crimes 'due to the invisibility and complexity of digital traces' [76, p.738]. In other words, deviant security is one of the reasons why there is little known about cyber criminals and their crimes. So besides legal practitioners, academics who (would like to) study organized cyber crime are limited to do so because of deviant security practices. Therefore, multiple participants' perspectives are sought during the inquiry [247, p.280], solely based on secondary data sources (see Section 4.1.2). The secondary data sources of this study are derived from research participants with experiential relevance, more specifically i) *those who apply deviant security* and ii) *those who are confronted with deviant security*, thus respectively cyber criminals - mostly computer-focused criminals, and to a lesser extent computer-assisted criminals - and participants, like legal practitioners, from the cyber security community.

Participants in cyber crime networks The focus of this study lies on active offenders (as compared to a prison sample) with the following characteristics in frequency, nature and severity of offending, and skill levels and abilities [251, p.6]. They are suspects of crime, and operate on their own and/or within loosely to highly organized groups that commit profit-driven computer-focused crimes with an international impact such as online banking fraud, ransomware and spam (see also [196] who had access to similar but less research data, and reviewed several of the same investigations). These groups are small with just a few members to very large, consisting of 50 to even more than 80 individuals as in respectively the cyber criminal Lurk and Dyre organizations [252][253].

Computer-focused criminals not only include end-user cyber criminals (those criminals who are at the end of the cyber criminal value chain and make victims), but also cyber-crime-as-a-service providers. The latter develop and offer various cyber criminal services and products that the end-user criminals need to commit and protect their financial cyber crimes such as malware, exploits, infected computers (botnets), and bulletproof-, code obfuscation-, credit card-, money mule-, and phishing services [254][255][256], see also Figure 6.2.

Cyber crime in networks and as a service
Because of their interdependence to succeed, cyber criminals form collaborative relationships that are characterized as cyber crime networks which evolve around informational capitalism [257], i.e., criminal assets that are further explained in Chapter 5 [34][258]. Information technologies empower criminals in commission and protection. Indeed, IT acts as a force multiplier, enabling criminals with minimal resources to generate potentially huge negative effects [28][78]. IT also allows a single criminal to commit a large number of small or low-impact crimes distributed among many jurisdictions [34]. Thus, IT promotes the deskilling and reskilling of criminal labour and collaboration among cybercriminals. These developments have led to cyber-crime-as-a-service (CaaS) economy - in other words, commoditized crimeware in the underground market [255] - including providers that deliver services/products for protective purposes. It is therefore expected that the organized nature of cyber crime will keep increasing in the future [76][259, p.7]. That cyber criminals and their businesses are networked becomes evident in the following case. Lurk was a malware that targeted Russian financial institutions. After members of this group were arrested in Russia, the Angler exploit kit - another specialized service - completely disappeared. Both groups were apparently highly interconnected, or perhaps even one and the same [260]. This *interdependency* poses a major vulnerability to cyber criminals and their crimes. For example, money mule herders have, according to Europol, a high dependency on the availability of mules and a medium dependency on fake identity documents (IDs) to open bank accounts [261] (see also [179, pp.31-32]).

Police evidence shows that committing financially-driven cyber crime is their day job and primary means of support. The precise geographical location of many of these anonymous cyber criminals is unknown, but the population consist largely of cyber criminals who presumably live in Europe, former Soviet Union states and the United States of America, and master Dutch, English, Romanian and/or East Slavic languages (Belarusian, Russian and Ukrainian). While automated translation software was frequently used, a group of linguists, translators and police investigators with an East Slavic background also helped to understand the language and subculture of the latter group. Nota bene, Russian is also the *lingua franca* for cyber criminals who are not located in, or citizens of, the Russian Federation, but the Commonwealth of Independent States (CIS), large parts of Central and Eastern Europe and Northern and Central Asia (more commonly referred to as Русский мир - ‘Russkiy mir’). The terms Russian-language and Russian-speaking in this study therefore refer to Russian citizens and citizens of the countries of the former Soviet Union, as well as citizens of other countries who have emigrated from the countries of the former Soviet Union to other parts of the world [259, p.3]. However, there is also a considerable group of participants whose true identity and whereabouts are known, especially when investigations led to the arrest and prosecution of suspects. Over 50 Chinese cyber criminal fora have also been reviewed with the help of a sinologist, but less extensive compared to the English-speaking and East Slavic cyber criminal underground economies.

The participants of this study were further supplemented by computer-focused thrill-seeking criminals and sexually-driven computer-assisted criminals. The first group mostly consists of a small number of predominantly young Dutch amateurs (also known as script kiddies) whose crimes are predominantly DDoS attacks and defacements of websites. They generally have a forum presence on open gaming and closed script kiddie fora, communicate via chat and email, and may meet offline (see Section 7.2). The latter group consists of mainly Dutch viewers, possessors, distributors and producers of child sexual abusive material. They are sexually-driven (only a single commercial distributor of CSAM has been studied), and their core business evolves around producing, collecting and sharing child abusive material with like-minded people. Although their security practices are less well documented by academics, investigative journalists and private security researchers, police investigators and their dossiers are useful sources to learn more about these hidden and sensitive crimes. CSAM users apply deviant security too, have a presence on dedicated CSAM fora, use chat to communicate, and may meet co-conspirers offline.

Generally, the offline identities of the cyber criminal participants are unknown. Of some, even their online identity (also referred to as moniker or nickname) is unknown, which means that only their criminal activities are known to the researcher. To conclude, the research population of this study that operate in cyber crime networks is very diverse: they commit different crimes, have different backgrounds, motives and skill sets, are on different fora, use different chat clients, et cetera, and are active in different time periods and duration over time.

Participants in cyber security networks The second group of participants that has experiential relevance in this study are those who are confronted by deviant security: academics, analysts, attorneys, diplomats, investigators, judges, legislators, policy-makers, private security researchers, public prosecutors and (victim) witnesses. Most of these participants work within CERTs, corporate security (i.e., cyber threat intelligence departments) of large private enterprises, cyber hotlines on e.g., e-commerce fraud, identity fraud and online child abuse, European and international analyses and coordination agencies such as the European Cyber Crime Centre (EC3) of the European Union's law-enforcement agency Europol and the Global Complex for Innovation (IGCI) of INTERPOL, dedicated cyber crime investigation units of national European and federal US law-enforcement agencies, internet service providers, non-governmental organizations (NGOs), financial institutions, ministries/departments/offices/secretariats of state, the private security industry, and universities [262][56][80, pp.88-89]. Other participants are those whose assistance is sought by the cyber security community such as victims, witnesses, netizens and general Internet users: they too are confronted by DevSec [80, pp.88-89].

Many participants are members of cyber security networks that evolve around informational capitalism and are composed of nodes that are 'interconnected in order to authorize and/or provide security to the benefit of internal and external stakeholders' [91]. These networks are trust-based with secrecy towards non-members as a default policy [35, pp.234-235]. These networks are formed along linguistic, geographical and increasingly geopolitical lines. This study includes first-hand experiences and insights of different networks, such as visits to private and public cyber security agencies (including law-enforcement-, intelligence and security agencies) in various European countries, the United States of America, the Russian Federation and the People's Republic of China; and participation in strategic and operational meetings of the Dutch Electronic Crimes Task Force (ECTF), Dutch Information Sharing and Analysis Centers (ISACs), the European Joint Cybercrime Action Taskforce (JCAT), the US International Cyber Crime Coordination Cell (IC4), and the US National Cyber-Forensics & Training Alliance (NCFTA). During such visits and meetings, agencies generally presented their strategies and/or finished and ongoing operations against profit-driven computer-focused crimes.

4.1.2 Secondary Data Sources

What kind of data sources are collected from these two participant groups? In qualitative inquiry in general, and Grounded Theory (GT) specifically, the researcher *is* the instrument [263, p.34]. Qualitative research (especially GT, but also the previously mentioned empirical legal scholarship) promote that the researcher should first become familiar with an area of scientific research that, in this case, is relevant to the development of law and policy, and should take a multidisciplinary approach to develop knowledge [230, pp.866, 871-875][239, p.41]. Entry into the field and locating participants are not an issue in this study as the researcher works within the cyber security community. As said, these networks are trust-based as trust facilitates the necessary willingness to share information [56][262]. Because organized crime is largely a hidden phenomenon that is only revealed with the use of evasive investigative powers [249], being an embedded academic researcher within a national law-enforcement agency that has a tradition in cooperating with academics in empirical research in the area of organized crime (or: a police investigator who is conducting scientific research) [264], opens more opportunities to collect rich secondary data sources about the two participant groups than working in a traditional academic setting.

Personal writings of cyber criminals Grounded Theory depends on qualitative field research to investigate those attitudes and behaviors best understood within their natural setting [265]. Although this study relies on typical qualitative data sources such as interviews, observations and documents [239, pp.129-143][247, p.274], there are also considerable differences with the common practices as prescribed by most literature on GT. The constructionist view on GT prescribes that researcher and participant should embark together on the process of constructing reality [243]. However, this study does not construct reality through interviews with those who apply deviant security as this decreases the number of available participants, and raises questions about the credibility of the researcher and a number of serious ethical issues. A criminal might provide (new) incriminating evidence about former or recent activities during the conversation. Dutch law prescribes that the interviewer, in this study being both researcher and police officer, is obliged to act when he/she suspects that certain crimes have been committed like explaining to the interviewee that he/she is a suspect of crime and has the right to remain silent. Instead, this study relies on unobtrusive information created by cyber criminals themselves, so-called ground truth data. Other researchers have done this as well, such as McCoy et al. and Kanich et al. who both used the operational databases of malafide pharmaceutical affiliate programs to understand their business [168][188]. In this study, not only such databases, but also chats, logs, postings, audio and video conversations are used. Cyber criminals largely communicate online, using social media, chat, email and fora to discuss - amongst others - security related matters [266][267]. Participants within the cyber security community - especially law-enforcement agencies - have both the legal, organizational and technical ability to gain an information position in the underground economy, either by intercepting data in motion or by preserving and/or seizing data at rest [20, p.207], as well as manually engaging in conversations with cyber criminals. Lawfully intercepted and preserved data of cyber criminals are unobtrusive. It therefore allows to observe cyber criminals in their natural setting which contributes to scientific credibility as these text-based data are created - i.e., mostly written - by the participants themselves. Other sources also ensure access to unbiased and non-contaminated data about the physical, offline environment of cyber criminals. The researcher has participated in house searches of cyber criminals, and reviewed photo images and video recordings that were made by LEA during undercover operations and before, during and immediately after arrests of suspects and house raids. So, compared to researchers who use a single source - a leaked client database or cyber criminal forum - this study uses multiple data sources that were generated by the cyber criminal community.

Participant observation Another data source is participant observation within the cyber security community. The idea behind participant observation is that certain experiences are only understood through an intensive involvement with the people in their cultural environment, usually over an extended period of time [250]. The idea of moving from research *on* the police to research *with* the police seems especially applicable to study cyber criminals and their practices [268][269, p.4]. Working as a researcher within the cyber security community provides opportunities to understand the full concept of deviant security. Daily proceedings within these cyber security networks evolve around being confronted with deviant security, and - when it concerns police investigation units - trying to breach that security to collect evidence. In practice, the researcher has frequently conducted (and thus experienced) the full investigative cycle within a European national cyber crime unit - i.e., the Dutch National High Tech Crime Unit (NHTCU) - that investigates complex, innovative and/or organized computer-focused crimes, mostly within an international context during this study (for an extensive description and evaluation of the cyber security and cyber crime discourse in the Netherlands in general and the NHTCU specifically, see [270][271]). The unit consists of over 120 individuals with various academic and police backgrounds. The NHTCU was - amongst others - involved in investigations against the following organized groups behind financially-driven computer-focused crimes with an international impact such as Buhtrap, Carbanak, Dyre, GameOver Zeus and Torpig, ransomwares such as Chimera, Coinvault, CTB-locker, Shade, Teslacrypt and Wildfire, and DDoS booter Webstresser.org [272]. The unit is also one of the initiators of the award-winning public-private platform No More Ransom to prevent, detect and confront ransomware [273], the No More DDoS platform to prevent, detect and confront DDoS attacks, and Hack_Right for alternative sentences - e.g., community services, financial transactions, fines, official warnings and probation - for young, low-threat offenders. The unit was further responsible for the takedown of multiple botnets, such as Bredolab and Simda, arrests of the individuals behind bulletproof hoster Maxided and related CSAM file-sharing service Depfile, and for the takeover and takedown of cryptomarket Hansa. Led by international partners, NHTCU was also involved in the investigations of the bulletproof infrastructure Avalanche, the cyber criminal forum Darkode and underground bank Liberty Reserve. Less known cases involved investigations against (mobile) banking trojans and other forms of online frauds, and a wide range of criminal facilitators such as malafide telecom providers and online money laundering schemes, including rogue cryptocurrency tumblers and job scam services. In a few instances, sexually-driven computer-assisted crimes were investigated as well, especially cases against high value CSAM targets. Data of all these investigations, and many more that remain confidential, were reviewed for this study.

During this five year research project, hundreds of conversations and informal interviews were conducted with participants from the cyber security community. Why so many interviewees? That is because police investigators continuously have many (and often long) discussions with the above mentioned participants as so much is still unknown about the commission and protection of cyber crime and related responses such as investigations, laws and policies. The individual interviews were taken by the researcher in his other capacity as a police officer. Only notes were taken during these conversations that varied between unstructured, open-ended interviews and semistructured interviews [248, pp.150-152][239, pp.130-134]. Group discussions in which results of this study were presented were conducted as well (basically member/stakeholder checking and focus group interviews [248, pp.194-206][239, pp.208-209][263, p.346]). Additionally, observational field notes were written about deviant security related issues that the researcher experienced himself during investigations as opposed to the participants' interpretation of the investigative events.

Data sources from participants in practice
Police investigations evolve around seeking the truth and making statements that go beyond reasonable doubt [274, pp.489-490]. Therefore, investigations generate trustworthy, credible and coherent data to reconstruct who is responsible for what, or - in case of ongoing crimes - what is going on and who is involved. Generally, multiple hypothesis are tested and a variety of data sources are used before conclusions are drawn. During an investigation of a high value CSAM target in the Netherlands in 2015, the Dutch National High Tech Crime Unit (NHTCU) worked with the Dutch National Child Exploitation Team and foreign law-enforcement agencies. The consortium placed wiretaps on telephone and Internet connections, preserved servers, installed recording devices in the suspect's car and house, conducted physical observations, gained a presence on CSAM fora, executed a house search, interviewed co-conspirers and witnesses. In another investigation into a computer-focused crime, the NHTCU received a report of a private security company. The report stated that several C&C servers were hosted in the Netherlands and used on attacks on financial institutions. Servers outside of the Netherlands were preserved as well. Furthermore, netflow, payments details and subscriber details were requested. The private security company provided further details about the MO, malware samples and used exploits, while Europol organized a meeting to inform all major European banks. The Dutch GovCERT - *Nationaal Cyber Security Centrum* (NCSC) - sent a threat analysis of the security vendor to national CERTs that further distributed this report to national banks. National CERTs and victims in turn, provided new information about the attacks as well. The NHTCU also collaborated with multiple governments, and received and made advanced analyses about offenders, used infrastructure and attacked victims.

Other sources Other used data sources include open-source files about deviant security such as academic studies, news media, non-fiction books, policy documents, security blogs and videos. Furthermore, legislation and policy documents were reviewed, especially from the Netherlands, and to a lesser account, the European Union and its Member States. Closed-source files mainly consist of police dossiers for court purposes, although a court judgment may not necessarily have been issued yet (see [196, p.4][249]). The latter files include obtrusive testimonies and (audio and video recorded) statements of suspects, witnesses and victims, and offline and online (unobtrusive) observations by law-enforcement officers [239, pp.130, 141]. An online open database of Dutch court documents was examined as well. Open and closed-source intelligence reports of public and private organizations about actors and threats, and confidential statistical analyses on criminal organizations and their crimes, used infrastructure and attacked victims were used as well. Such advanced analyses include timelines of botnet C&C IPs and domain names, patterns in ATM usage by money mules, network-actor models on intercepted chats, and social network analyses of fora, and were mostly produced and visualized by software programs as iBase/Analyst's Notebook, Gephi, Kibana, Maltego, yEd and/or VUE, and by tools developed by the Dutch national police and the broader LEA community. Furthermore, two questionnaires and a case study were distributed among police investigators in various countries for the European Multidisciplinary Platform Against Criminal Threats on cyber crime (EU Policy Cycle EMPACT), followed by a round table discussion with high level management of national cyber crime units (see Chapter 8). So, this study uses information that ranges from soft intelligence to solid evidence about deviant security practices [249].

These multiple qualitative and quantitative sources of data allow triangulation and strengthen validity, reliability and credibility [263, p.350][275, pp.233-234], which are important in cyber crime research [251, p.17]. Lastly, a small number of reflexivity journals are written about the researcher's own interpretations of the data as well as the feedback of the cyber security community participants on the constructed deviant security concepts (i.e., member checking [248, p.205]) [276][243, pp.131, 188-189].

4.1.3 Data Collection, Analysis and Writing

How are these secondary data sources collected and processed for research purposes? A central characteristic of GT is simultaneous collection, analysis and writing which are considered interrelated processes [246, pp.419-420][277, p.34]. For explanatory purposes, this section distinguishes between and describes how the initial data collection and analysis were executed, and how subsequently constructed categories were refined with the help of theoretical sampling.

Initial data collection and analysis A total of five years was spent in the field, and during that time, relevant secondary data sources were collected in the following sequence. Firstly, the topic was observed and experienced during police investigations without collecting data. This helped to get acquainted to the field in general, and specifically to the cyber security community and police culture, daily work proceedings, and available data sources. After this adjustment and exploration phase, the initial coding and data collection started. This study first applied deterministic, purposeful sampling methods which focus on selecting information-rich cases and participants [278]. Participants and cases were sampled opportunistically, based on their availability to the researcher (convenience sampling) [279, p.28]. Because the cyber security community and their investigations are networked (meaning that many nodes within the network will contribute to, or at least become aware of, transnational cyber crime cases), and because criminal infrastructures are often hosted in the Netherlands, the researcher was continuously notified by public and private actors about new and ongoing high profile cases. Cases were also generated by his police unit, because of reactive investigations (e.g., based on a victim complaint) and proactive investigations (based on own initiative). At the same time, data were also collected from open sources, mostly blog posts from security researchers (nota bene, evidence from open sources is also collected during police investigations). Participants within the cyber security community who were aware of the research project further pointed to cases that were interesting to review. Especially former CSAM investigators that switched to computer-focused investigations pointed out relevant online child sexual abuse cases.

The DevSec-related issues in these sources were written down, then initially coded and later focused coded, i.e., extensively testing the most useful initial codes against other data on a low level of abstraction [243, p.43]. These codes were subsequently linked to either the *what*, *who*, *when and where* of deviant security or a rest category in NVivo. DevSec suppliers on fora were linked to *who,* while instances of encryption were initially linked to the rest category, only to realize later in time that cryptography is linked in this study to time, thus *when and where.* Simultaneously, informal analytical notes (memos in GT terms) were written about the ideas that occurred. Slowly, the first preliminary categories emerged.

A day in the office: continuous cycle of data collection & analysis
Generally, the progress of ongoing investigations is discussed on a daily basis within the Dutch National High Tech Crime Unit. Setbacks and break-throughs in investigations respectively mean encountered deviant security practices or exploited vulnerabilities such as a successful wiretap, a match between an email address and nickname, the preservation of a C&C server hosted in the Netherlands, or an official police report of the criminal intelligence unit about the real identity of an unknown (so called no name) suspect. As in qualitative research, data collection is followed by the analysis phase in investigations. On many occasions, the data is too abstract, and multiple perspectives - digital, financial, tactical - are needed to make sense. What are we looking at? Does this link to any existing entities or other pieces of information? Which hypotheses do this data confirm or reject? Why would the individual behind this attack use this tool? Is this disinformation or did the perpetrator(s) really make this mistake? Which investigative power should we execute next? Essentially, these discussions were often implicitly about filling in the various components of the deviant security process cycle. Frequently, the help of others was sought. When legally allowed, a combined analysis was done with private security researchers who were studying the same malware campaign, foreign LEAs who were conducting parallel investigations, and increasingly academics as well. A new phase of data collection and analyses would start. Besides investigations, analyses were conducted about the broader cyber threat intelligence picture and to determine long-term cyber security strategies. Is this particular ransomware on the rise, and if so, where are perpetrators, infrastructure and victims located? Who are the key enablers within the CaaS value chain? What are the downsides of virtual currencies for both the cyber criminal and investigative business processes? How do we inform 20.000 malware victims that are located all over the world? Which academic, private industry or public sector collaborations do we need to deal with this particular problem? What is our approach to country X, international organization Y and newly founded cyber security platform Z? We have found a criminal database of a DDoS service with clients of a young age, how do we deal with them? Due to these discussions and experiences, the theories of deviant security were applied, tested and refined to understand the cyber criminal landscape and explore appropriate investigative responses.

Refinement of categories and theoretical sampling Questions arose and gaps appeared in these first categories. For example, there were many cases in which cyber criminals applied deception, but the deception tactics seemed to differ greatly. Two main categories emerged from the data: instances in which cyber criminals used deception to commit crime, which has protective side effects against law-enforcement; and instances in which cyber criminals applied deception solely for deviant security purposes. Still, within these categories, deception classifications were absent. A review of academic literature provided a useful taxonomy with various deception tactics. Many observed cases fitted within an adapted and enriched version of this taxonomy, although some of the described tactics had not yet been observed. More data was gathered - known as theoretical sampling - to fill in these gaps and refine the deviant deception framework and its properties. Examples of deception tactics derived from the literature were sometimes in the data set of this study, but not recognized as such till then. As with all categories in this study, theoretical sampling was further done by searching for data in police systems - a review of case files - as these systems perfectly lend themselves for quick, focused and easy keyword searches, while at the same time providing new and rich empirical data. In few instances, academic courses were followed on intercultural communication, international relations and Russian security policies, taught at universities in the Russian Federation.

It further became apparent that there were relationships between core categories across the study [243, pp.117-118]. Deception is, for instance, one of the causes for i) information asymmetries within ii) intertwined networks. As countermeasures against deception, cyber criminals apply iii) distrust mechanisms and iv) trust mechanisms. These four core categories are all linked to the *who* of DevSec, and as such it becomes apparent that deviant deception is best understood as an interactive process that occurs between key players of DevSec. At the same time, deception is also linked to the *what* of DevSec. Deception skills are an intangible asset to cyber criminals and punishable under substantive law. This insight helps to construct what makes security deviant, and define its basic normative and empirical qualities. These findings were used during informal group discussions with colleagues and other law-enforcement officers, while simultaneously receiving feedback, new ideas and further refinement of core categories. Such sessions were also helpful to test if categories were matured to a point in which saturation was reached and further sampling was not needed [243, pp.113-115]. Slowly, an integrated and comprehensive grounded theory on deviant security practices emerged that is placed within the sociological grand theory of the Information Age and explained by a combination of microeconomics and technical computer security.

4.2 Explanatory: Information Age & Microeconomic Theory

Two economic perspectives are used in this study to provide explanatory power. Firstly, deviant security practices are understood and placed within the larger sociological paradigm - 'the fundamental models or frames of reference we use to organize our observations and reasoning' [265] - of the *Information Age*. This perspective deals with the *macroeconomic* changes from an Industrial Age to an Information Age with economies based on information technology that essentially created cyber crime. The second perspective, *microeconomic* theory, helps to understand the decisions that cyber criminals have to make about some of the observed deviant security practices in this study.

4.2.1 Deviant Security in the Information Age

Similar to studies about the commission of cyber crime, the results of this study about the protection of cyber crime and the cyber criminal are placed within the grand theory of the Information Age. This section first explains the importance of having a framework that connects the macro, meso and micro level relationships that shape deviant security practices, and proceeds by briefly outlining why the paradigm of the Information Age is able to do so.

Placing a theory on deviant security in a social paradigm Why deriving categories *within* a larger conceptual framework as the Information Age, while Grounded Theory is essentially about developing new conceptual frameworks? First of all, Grounded Theory does not reject the use of existing theoretical frameworks if a theory complements, extends or verifies findings, or provides insights and directions for middle-range theories [240, pp.39-41]. This study about the security practices of cyber criminals is essentially a middle-range theory that fits within the larger sociological paradigm of the Information Age, and several concepts derived from that paradigm - like the importance of networks in today's society - add to a more granular understanding of DevSec. Strauss and Corbin further recommend to specify 'those conditions and consequences, at every level of scale from the most "macro" to the "micro," and integrating them into the resulting theory' [247]. So, they advocate to research the processes of society at large that influence and shape a research topic. The relevance for this approach is most striking in Chapter 7: deviant security practices are heavily affected by events outside the cyber criminal's sphere of influence. GT also promotes to study issues at the level of networks, small organized groups and individuals, more specifically for this study the deviant security of cyber criminal networks, groups and individuals, and cyber security networks, investigative units and individual police officers. As shown throughout this study and as visualized in Figure 4.1, the Information Age is able to integrate the macro, meso and the micro dimensions that shape DevSec.

Secondly, explicitly mentioning a social paradigm is further necessary because of *reflexivity* - the awareness of the researcher of how his/her world view, social identity and background impacts his/her study - which is of great importance to Grounded Theory [243, p.132][276]. Computer scientists and legal scholars generally do not explain to their audience what their perspective is on reality [234][280]. However, social paradigms have undoubtedly, but perhaps unknowingly, a profound impact on the outcomes of their research. Legal scholar Orin Kerr stated about research on Internet law:

> 'By choosing the perspective, we choose the reality; by choosing the reality, we choose the facts; and by choosing the facts, we choose the law' [281, p.361].

If that were so, both the researcher and his/her audience should be well aware what that perspective on reality is as, in this case, the research findings aim at impacting the decisions of legal practitioners in the public sector.

Deviant security in the Information Age The Information Age is a powerful paradigm to understand the macro conditions that impact the deviant security practices in the cyber criminal's micro environment. Although few computer science studies in general, and technical computer security studies specifically, refer to the Information Age, the perspective has been widely acknowledged by social scientists (like David Wall, Majir Yar and Myriam Dunn Cavelty [84][34][28][75]) and legal practitioners (of e.g., the Dutch national police [282]) as *the* paradigm to understand the commission of today's cyber crime and explore appropriate responses.

Amongst other scholars, sociologist Manuel Castells wrote an extensive trilogy about the social, economical, cultural and political transformations at the end of the previous century that have such an impact on today's life [45][283][44]. The strength of the paradigm for this study lies in its emphasis on the dominant role of information technologies in present day's society. Today's societies embrace, and indeed, depend so much upon IT, and its subset of the Internet, that Castells names this era the Information Age:

> 'Technology is society, and society cannot be understood or represented without its technological tools' [44].

Technology has accelerated globalization, and enabled the organization of dominant functions and processes within society around networks. Hence, present-day society is labelled a *network society* [44], which is vital for this study with its usage of secondary data sources of participants from cyber security and cyber criminal networks. The Information Age and Network Society not only have a profound impact on law-abiding entities, but also on the way today's crime manifests itself. Cyber crime is transnational, technology-driven and has become 'an essential feature of the new global economy, and of the social/political dynamics' [283]. As shown in Part III, the paradigm helps not only to understand the commission of cyber crime, but the deviant security practices of cyber criminals as well.

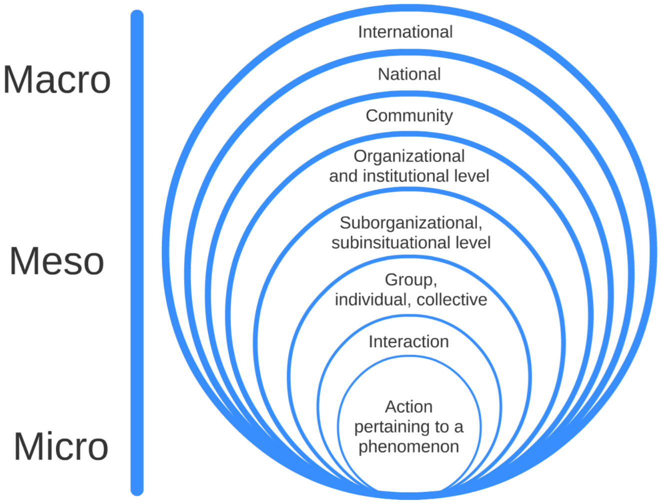


Figure 4.1: The conditional and consequential matrix, brought forward by Corbin and Strauss, is according to Charmaz 'an analytic device for thinking about macro and micro relationships that might shape the situations the researcher studies' [247, p.274][243, pp.118-119]. The security practices of cyber criminals are affected by interacting macro, meso and micro level spheres of influence. The macro (external) environment is uncontrollable to the cyber criminal, but have a powerful impact on his/her business and security practices. Macro level dimensions that affect DevSec include international and national laws, policies and law-enforcement interventions, but also technological innovations and societal events on which cyber criminals have little influence. Meso level spheres of influence point to DevSec-related aspects that occur within, or because of, cyber security and cyber criminal networks, like security culture on cyber criminal fora and other large collectives. Lastly, micro level refers to the individual factors of a cyber criminal that impacts his/her security, like learning capabilities, adaptability and other competencies. Figure 7.1 is a filled-in conditional and consequential matrix that presents the key concepts that shape the temporal-spatial nature of deviant security.

4.2.2 The Microeconomics of Deviant Security

Because Section 3.1.4 already explains attacker economics and the economics of deviant security, this section briefly discusses several underlying assumptions. Cyber criminals wittingly or unwittingly conduct i) *risk assessments* which are explained in this study by ii) *microeconomic theory* based on iii) *rational choice perspective*. In practice this means that the core categories of Part III are structured by principles from technical computer security, and further enriched by microeconomic theory to gain an in-depth understanding of the deviant security practices. Yet the formulation of investigative responses against deviant security cannot not solely rely on microeconomics, but also has to connect to the world of legal practitioners. In other words, effective police responses from a purely microeconomic perspective do not equal appropriate police responses from a legal point of view. Formulating appropriate responses against deviant security, including an assessment of the legal feasibility of investigation strategies, fits within the discipline of iv) *law and economics* - the application of microeconomic theory to analyze laws, policies and police investigations for a legal practitioner audience - and is very much the legal tail of this study.

Deviant security risk assessment Many deviant security practices can be explained by risk assessments that cyber criminals have to conduct. Cyber criminals hypothetically have to assess the risks that they face properly, not to a compliance standard of due diligence and due care (known as checkbox security), but because their physical and psychological integrity is at stake: they can get arrested, prosecuted, convicted and incarcerated for their crimes. Risk assessments should provide - amongst others - cost-benefit analyses (CBA) [59, p.74]. Yet the goal of this study is not to create a rigorous deviant CBA taxonomy, but rather highlight exemplary costs and benefits of the protection of crime and the criminal. These costs and benefits of this study are expressed in a qualitative manner such as, but not limited to, economic tradeoffs - the balance between various factors related to deviant security that are not attainable at the same time. Together with other microeconomic concepts that are mentioned in the next paragraph, these insights provide an understanding of the risks that cyber criminals are willing to accept - i.e., their risk appetite - and identify situations in which they apply e.g., too much or too little security.

Microeconomic theory Readers may notice that several key concepts of deviant security - such as trust [284, pp.572-573][54][285], assets [286][274], and temporal and situational factors for decision-making [287, pp.116-117] - are linked to microeconomic theory and rational choice perspective. Microeconomics is generally used to research economic activities as an interaction of individuals pursuing their private interests and allocating their resources in a market [70, p.5][286, p.3]. This research project is no exception, yet takes the practices of law-breaking individuals who operate on cyber criminal markets (i.e., attacker economics) as objects of study. As the little brother of the economics of information security [182][181], and previously explained in detail in Section 3.1.4, the core argument of the economics of deviant security is that not only the technical computer security practices of law-abiding agents but also those of malicious agents can be explained by microeconomic language such as competitive (dis)advantages, information asymmetries, negative externalities, perverse economic incentives and tradeoffs.

Rational choice perspective The use of basic microeconomic theory to understand e.g., security tradeoffs assumes a rational choice perspective (RCP) [54][288, pp.4,8,47]. RCP on crime was originally put forward by the academic discipline of crime science, and takes the offender's decision-making as the central focal point for understanding criminal behavior [289][209]. Lately, the perspective has also been deployed on cyber crime [290][291][292][293, pp.581-582], and adopted by the discipline of cyber crime science (CCS) [288]. The latter discipline advocates RCP for interventions that immediately reduce the commission of cyber crime and harm to victims. CCS combines technical computer security with empirical research methods used in crime science which are similar to grounded theory data collection principles and techniques such as triangulation, direct observation, and interviews [288][289][294]. Rational choice assumes that criminal behavior is a purposive, dynamic process influenced by situational factors in which offenders try to maximize profits and minimize risks. RCP further assumes that criminal behavior is rational in the sense that offenders may improve their decision-making through experience and learn and modify their strategies to commit crimes, albeit bounded by limits of time, ability, and the availability of relevant information (also known as bounded rationality) [295, pp.1-2][296, pp.24-36].

Law & economics Microeconomic theory based on rational choice provides explanatory power to the DevSec model, but also forms the tailpiece that connects to the legal significance of the study. Not only prosecutorial discretion, plea bargaining and sentencing discretion may be understood in economic terms [297], but aspects of criminal procedure prior to prosecution as well, such as police investigations. Offensive investigative powers stand in close relation with the vulnerabilities and tradeoffs of the cyber criminal. More specifically, they try to exploit them and breach the cyber criminal's security system. Therefore, they are very much economically-based instruments that work as an incentive for cyber criminals to change their behavior, and to increase the efficiency of responses [274, pp.5-7][298]. Their investigations further have to collect evidence that prove that criminals have acted rationally [274, pp.501-502], while taking into account levels of bounded rationality, i.e., cases where there is no or less culpability. Because of this economic approach, the last chapter of Part III includes implications for legal practitioners, and fits within the legal discipline of law and economics [299]. This discipline is a subfield of ELS when a study is based on empirical data and not merely theoretical [235, pp.145-146].

4.3 Limitations

As the first structured and systematic research project on deviant security practices of cyber criminals, this study has inherent limitations of its participants and empirical data, methodology, theoretical foundations and outcomes. This section reflects on the nature of these limitations, provides arguments for the choices made and suggests how such limitations could be overcome in the future.

Participants and empirical data Limitations concerning participants and related data sources are plentiful. Firstly, there is a lack of knowledge about financially-driven computer-focused criminals who are so successful in their DevSec practices that they remain undetected. For example, a top law firm stated during this study that they frequently had quoted companies as clients who were hacked, whose confidential files were stolen and who were subsequently extorted. During the five years of this study, not a single organized extortion group was discovered, until the last year of the research project. How many more cyber criminal schemes are out there, not yet detected by or reported to organizations with a public mission like the academic world, law-enforcement agencies or media outlets? There is evidence that some of the top organized computer-focused criminals are physically working together to limit the amount of online communications between group members. While we sometimes see their damage to victims, large parts of their MO - especially their preparations, pre-activities and post-activities - are shrouded in mystery. Moreover, this study relies on information that ranges from soft intelligence to solid evidence, including third party intelligence reports and lawfully preserved and/or intercepted writings of anonymous individuals who - amongst others - discuss DevSec practices. It is difficult to check the underlying sources of these reports, while reality can turn out to be rather different from what initial investigative steps suggest [249]. A third concern with some of the solid sources is the lack of corroborating evidence to check if the referent objects concerned also (correctly) implemented the discussed DevSec policies and mechanisms in practice. Furthermore, it is unknown to what extent encountered countermeasures of this study's participants can be generalized to other cyber criminal communities. Few controls were only observed a single time, while *the* cyber criminal community does not exist. It is unknown how accepted and how frequently these countermeasures are also applied by others, like Brazilian politically-driven hacktivists [300], as cyber criminals and the networks to which they belong, are very heterogenous, and differ in culture, motives, skill sets and so on. Lastly, the described and explained deviant security practices might be a snapshot in time. Although the DevSec policies and mechanisms are described on a high level of abstraction, we have no idea how controls of cyber criminals will develop over time as this is the first major study on these practices. Yet the quality and quantity of participants and empirical data of this study is unprecedented compared to other academic studies. Moreover, the goal of this study is to present a first broad overview of the various components of deviant security, and more research is indeed needed to address these limitations. Therefore, each section ends with an interim conclusion and discussion that lists directions for future research.

Grounded Theory A concern related to the methodology of GT is the possibility that the normative outcomes and constructed categories of this study are regarded as non-objective, non-critical or biased as the author is working within the cyber security community. As stressed by others, 'innovative research methodologies, including direct engagement with law-enforcement, forum participants and observations of market activities before, during, and after any intervention' are needed to explore effective responses [301, p.97]. Besides documented problems related to research with police such as cultural and organizational barriers [268], advanced investigations on computer-focused and computer-assisted crimes are lengthy, progress in irregular fashion with uncertain outcomes, and take place in very closed, trust-based environments. Academics might not have time, or even have the opportunity, to deploy such innovative methodologies. So being embedded within law-enforcement might be inevitable to study deviant security in detail. Still, this study invested in overcoming the above mentioned objections by refraining from securitization and commodification of security. Whether scholars apply Grounded Theory or not, awareness of their own preconceptions, values and beliefs is vital as security is indeed increasingly deeply political [302]. Moreover, results of unsupervised statistical and artificial intelligence methods and techniques such as word2vec and topic modeling on cyber criminal data also steered the direction of this study. These methodologies perfectly fit within Grounded Theory as they promote the unbiased discovery of theory in large data sets. Yet the potential and limitations of applying such technologies in GT need further exploration. Lastly, some scholars might conclude that this research is not a true Grounded Theory study, or a too flexible interpretation of the methodology especially as a mixed GT approach is used in this study, existing theories to explain deviant security practices and a literature study was conducted in Chapters 2 and 3. However, several scholars, including Strauss, Corbin and Charmaz, have argued that researchers should not rigidly apply Grounded Theory, but with a degree of flexibility and creativity instead [303, p.7][245, p.77][243, pp.2, 9].

The Information Age Manuel Castells' trilogy has been named as belonging to 'the class of grand sociological grand theory' [304]. If this is true, remains the question. On the one hand, Castells has been criticized for extrapolating from current trends, and using empirical data selectively to make normative arguments [305]. According to Castells, the European Union would be the best example of a successful decentralized network of 28 states. Yet he overlooks the constant push of the EU, including Europol and Eurojust, for more influence - i.e., centralization - upon the area of cyber security and cyber crime at the expense of Member States [306][307][308][309][310]. Related to this issue is Castells' position on a grow towards globalization instead of the traditional nation-states. Yet we see the revival of nation-states - i.e., China, Russia, United Kingdom and United States - and new geopolitical blocks which have a true impact on the fight against cyber crime as Section 7.3 shows. On the other side, when the first volume was published in 1998, a critique was that much of the work was pushing at open doors [311], such as the importance of information technologies and networks in today's society.

A problem for this study is further that Manuel Castells did not mention cyber crime at all, but solely discusses organized traditional crime in the Information Age. Yet cyber crime significantly differs from traditional crime, pressing the need for new academic disciplines such as cyber criminology and cyber-crime science [204][288]. Notwithstanding this argument, several leading criminologists on cyber crime, most notably David Wall and Majid Yar, successfully used the paradigm to understand financially-driven computer-focused and sexually-driven computer-assisted criminals. Still, the question could be raised how deviant security would fit within other grand theories. Deviant security could also be placed within grand sociological theory of the Risk Society, as described by Ulrick Beck, David Garland and Anthony Giddens [312][313][314]. From this perspective, more emphasis would be on risk as compared on (deviant) security, and the interplay of risk as a source of insecurity and related risk management for both cyber criminal and cyber security communities. Such an approach would research how the attacker capabilities of key players from both communities create risks and uncertainties for the other side and fuel each other's insecurity that have to but cannot fully be governed.

Economics of Deviant Security A first limitation about the microeconomic explanations of this study is its merely qualitative and inductive nature, as compared to deductive and quantitative. While (unpublished) statistics are used as data sources as well, a more mixed methods approach on the economics of deviant security would produce more robust outcomes. Yet the goal of this first structured and systematic study on DevSec is to show that economics is a helpful discipline to explain some of the encountered security practices of cyber criminals. A shortcoming related to microeconomics and rational choice perspective as theories to explain deviant security practices is the critique that people are boundedly rational, fail to maximize their utility and that their preferences are affected by context [315][316, p.39][317]. For research on cyber crime specifically, RCP would lean too much on the notion of human behavior as the driving force behind criminal activities, and too little little on the hybrid partnership between technology and humans, especially in crimes that have a robotic and automatic character such as botnets [293, pp.581-582]. However, applying microeconomic theory and a rational choice perspective in this study - supported with empirical data and build upon a grounded conception of DevSec - pays attention to those shortcomings and is more sensitive about context. These first law-and-economics insights might ultimately fit within a wider law and behavioral science movement that researches deviant security as a field of study on its own and supplements the inadequate elements of the RCP with insights from other social science disciplines [315]. Indeed, there is a need for new perspectives, such as the anthropology, linguistics or psychology of deviant security that will provide more explanatory power and broaden the field of study.

Outcomes for legal practitioners A limitation of this multidisciplinary study is its review of predominantly Dutch normative data sources, i.e., legislation, policy and investigations, even when some of the reviewed operations are conducted by other countries. For instance, when other countries send a request based on a mutual legal assistance treaty (MLAT) to the Netherlands, the national police of the Netherlands opens a criminal case under Dutch law to execute the request. A concern with research in such complicated socio-technical-legal settings is that the researcher is thrown back to his/her own cultural prejudices and internal feelings [109, p.95]. This indeed occurred, for example, during presentations and collaborations with officers from several national and international law-enforcement organizations. While more comparative legal research on cyber crime in general and deviant security specifically is indeed needed, this study is the first that has access to and takes notice of views of multiple law-enforcement agencies from various non-Western jurisdictions. A further criticism might be the relatively small audience of legal practitioners, even within a single legal discipline, more specifically criminal law [234, pp.425-426]. Yet this study focuses on *all* legal practitioners within the criminal justice system as compared to merely lawyers. Nowadays, the former occupational group includes many professionals with a technical background such as data scientists, digital investigators and software developers, and with a social science background such as behaviorists, criminologists and statisticians. Moreover, the multidisciplinary nature of this study will appeal to a broad audience and is a representation of what cyber crime and investigations truly are. Both phenomenon and reaction to this phenomenon are socio-technical practices within respectively substantive and procedural legal frameworks.

One might further argue that this study adds to the process of securitization by overly focusing on the administrative, physical and technical security practices of cyber criminals, and related investigative responses that are part of the border-centric view on cyber security and cyber crime. Firstly, the security practices of cyber criminals are viewed in this study from a technical computer security perspective (as compared to responses that are viewed from a cyber security perspective). According to scholars from the Copenhagen School, this technical discourse does not qualify for securitization [4, p.1160]. Simply put, securitization is very much out of the question when describing and explaining the phenomenon of deviant security practices from an academic, technically neutral point of view. Although suspects of cyber crime and their security practices have always been a core domain of public policy, law and investigations, the pitfall of securitization is real in the debate about *investigative responses* to deviant security. After all, scholars of the Copenhagen School argue that securitization language is frequently used in cyber security [75] [107][30][4]. For this reason, the research project refrains from securitization grammar, and does not - amongst others - qualify and/or quantify how big a threat deviant security is to investigations, nor pleads for expansion of investigative powers. The Copenhagen School's securitization approach itself also has serious shortcomings. It has been criticized for being merely an analytical tool with limited normative utility [318]. In other words, besides simply arguing for desecuritization, the analysts that apply this approach have little 'ability to influence the securitization process in a deliberate and thought-out fashion and [...] to a desired effect' [318, p.44]. Therefore, this study presents a normative framework against deviant security in Chapter 8, taking notice of the critiques of the borderless view on cyber security and cyber crime by regarding police investigations as means to provide human security that respect Internet as a global public good.

4.4 Ethical issues

This study not only tries to avoid ethical problems - e.g., harm to participants - by installing safeguards for those who apply deviant security, but also for those who are confronted by it. Contrary to other studies on cyber crime [319], the research project has explicit academic Research Ethics Board approval from the University of Bristol, and legal approval by relevant government authorities in the Netherlands based on the Dutch Police Data Act (*Wet Politiegegevens*), to use the previously mentioned secondary data sources for research purposes and publish about the deviant security practices of cyber criminals.

Protecting those who apply DevSec During data collection, there was *no* offline or online interaction/contact between the researcher and the cyber criminal participants *for the purpose of this study.* Only secondary data sources are used. Several measures are taken to ensure their anonymity during data analysis and writing. Firstly, detailed information in this study is predominantly derived from legitimate sources on open, public sources such as newspaper articles and technical reports from investigative journalists and private security researchers. Illegitimate sources that have been leaked online are not used, to prevent revictimization. When it concerns information derived from closed sources like lawfully intercepted communications of cyber criminals, the vast majority of offline identities of the cyber criminals are unknown to the researcher for the simple reason that these individuals are not identified because of - amongst others - deviant security. Secondly, the method of data analysis and writing - inductively developing a theory as prescribed by GT - ensures that constructed DevSec policies and mechanisms are quite abstract and not linked to the true identity of those who apply deviant security controls. The latter argument also applies to those cases in which the offline identity of the criminal is known to the researcher (especially police reports). For this reason, the use of quotations to bring in the voice of these particular participants is missing [239, pp.182-183]. While outsiders will have a hard time in attributing the de-anonymized cases to individuals, potential harm may still occur when insiders justly and/or erroneously recognize themselves or others.

Protecting those who are confronted by DevSec During data collection, there was *no* offline or online interaction/contact between the researcher and participants from the cyber security community *for the purpose of this study.* Conversations and interviews with these participants are also considered secondary data as these were conducted as an investigator who worked on operational cases and in need to understand DevSec practices that are thwarting investigations. There are also other ethical considerations to protect those who are confronted with DevSec and their daily proceedings. Individuals in the cyber security community - most notably, private security researchers and investigative journalists - have been threatened by cyber criminals in the past. It is a myth that cyber criminals are merely 'tech geeks' who will refrain from using violence against persons they deem threat agents. There have been instances in which cyber criminals use physical violence, including the use of fire arms, against law-enforcement officers. Therefore, research findings are presented in such a way that they not harm participants from the cyber security community. These considerations also apply to the community's capabilities to fight crime. Cyber criminals collect and exchange information about law-enforcement activities [320, p.18], and one of the findings of this research is that cyber criminals benefit from understanding the capabilities of their threat agents. So, not only quotations of interviewees are missing in this study, but also screenshots of fora, names of police operations and writings that link LEA to specific investigations, unless these findings are also found on open Internet sources. Thus in many instances, this study cites publicly available sources, although the researcher had far better operational insights. Citations are in this study also used as references for readers to learn more about certain public and private operations against cyber crime. This practice indeed differs from other qualitative studies which present such direct observations to enhance their credibility to their audience [248, pp.414-417].

Lastly, some people might believe that this study in general will benefit cyber criminals in building better security and therefore harm police investigations. Ross Anderson points out that this issue has already been addressed since the first books on cryptography were published around the 16th century. When he addressed the question if his book on security engineering should be published at all, Professor Anderson commented [36, p.xxviii]:

> 'While some bad guys will benefit from a book such as this, they mostly know the tricks already, and the good guys will benefit much more'.

While he referred to knowledge that might help the commission of crime, the same reasoning applies to knowledge about deviant security. The cyber criminal community already knows all the tricks in this study about the protection of crime: deviant security is frequently discussed at great length on cyber criminal fora, and many data are collected from similar closed and open sources. As pointed out above, many studies are also not police investigator-centric, while poor knowledge and skills of police investigators prove to be the reason for ineffective investigations [321]. More research on the specific problems that investigators face will increase the effectiveness of their investigations, and deviant security is definitely one of these problems. Lastly, the inductive inquiry of this study allows a level of detail that illustrates the underlying principles of DevSec, rather than being a handbook for cyber criminals.

Part III

Research Findings

Chapter 5

What? - Basic Qualities of Deviant Security

The next chapters present the core categories of the technical computer security practices of predominantly profit-driven computer-focused criminals that stand out in the data, and are considered the most relevant to legal practitioners. The core categories that are presented in this chapter follow the narrative account of criminal investigations setting out who did what, when, where, how and why [322, pp.256, 269][323, p.308]. More specifically, *how* cyber criminals apply protection is understood in this study by researching:

- *What* are the basic normative and empirical qualities of DevSec (Chapter 5);
- *Who* are the key players and related interactive protective qualities (Chapter 6); and
- *When* and *where* is DevSec applied, i.e., temporal-spatial protective qualities (Chapter 7).

When looked at the bigger picture, the findings of this research suggest that cyber criminals need to protect anything, against anybody, anywhere, at any time. As a consequence, they constantly (have to) make cost-benefit analyses about their security that can be understood in - amongst others - microeconomic terms. Therefore, all chapters provide explanations:

- *Why* security-related practices occur, in other words, reasons for observed deviant security practices. These explanations are mostly derived from the economics of deviant security - a combination of technical computer security and microeconomics - and to a lesser extent other social science disciplines such as linguistics and security studies.

The sum of observed deviant security practices represents the full range of administrative, physical and technical countermeasures of a preventive, deterrent, detective, corrective, recovery and compensating nature. The identified deviant security policies and mechanisms in this study should, however, not be considered in isolation, but in close coherence as depicted in Figure 9.4. Cyber criminals very much apply security in compensating layers. More precisely, they have their own version of defense *and* offense security in-depth, aimed at protecting the criminal and his/her crimes against threat agents.

The first research question is an obvious one. The term is used throughout this study, but *what* exactly *is* deviant security? A multidisciplinary approach answers this question. Concepts derived from computer science, and more specifically technical computer security, are at the heart of this chapter, and subsequently combined with concepts - see Figure 5.1 - from various other academic disciplines. Legal scholarship helps to *define* deviant security; security studies to understand the *meaning* of DevSec; and microeconomics to explain the *provision, form* and *function* of the security of cyber criminals.

Technical computer security to understand DevSec practices
This study categorizes DevSec as being either *defensive* or *offensive* in nature, and as *administrative*, *physical* and *technical* security controls [59, p.28]. The conceptual differences between these categories are illustrated by the following observed case. An email service was advertised as a high security web-based email system with encryption, authentication, public key infrastructure (PKI) and Secure/Multipurpose Internet Mail Extensions (S/MIME). For this reason, many cyber criminals were attracted to this service. The bad guys made, however, one mistake. The email service only offered technical security, and *not* administrative security against information requests of law-enforcement agencies. On the contrary, the company fully complied to court orders. While a copy of the content of the mailbox cannot be extracted, valuable metadata can be successfully delivered by the email service.

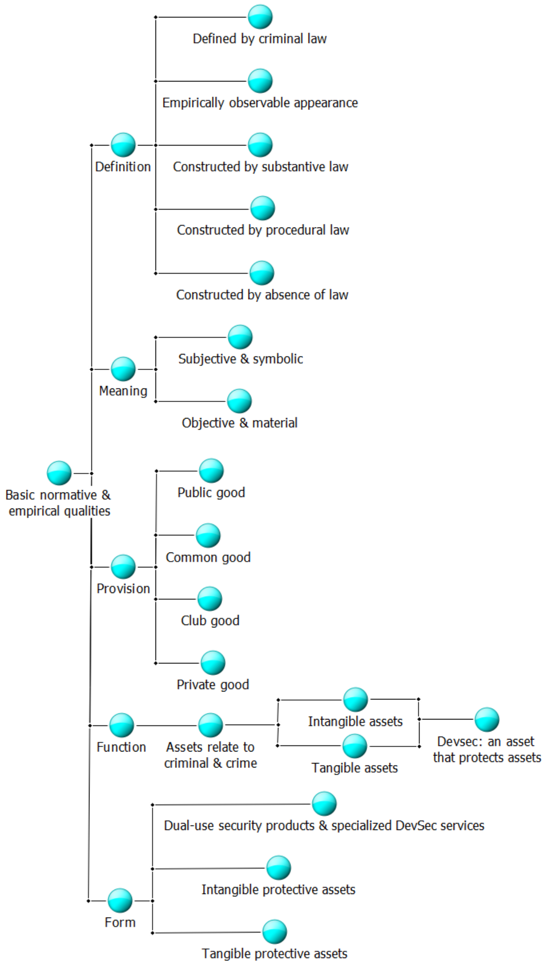

Defined by criminal law
Empirically observable appearance
Definition
Constructed by substantive law
Constructed by procedural law
Constructed by absence of law
Subjective & symbolic
Meaning
Objective & material
Basic normative & empirical qualities
Public good
Common good
Provision
Club good
Private good
Intangible assets
Function
Assets relate to criminal & crime
Tangible assets
Devsec: an asset that protects assets
Dual-use security products & specialized DevSec services
Intangible protective assets
Form
Tangible protective assets

Figure 5.1: This oversight visualizes the structure of Chapter 5 via a selection of key concepts about the basic normative and empirical qualities of deviant security. For a full oversight of descriptive and explanatory key concepts of Part III and their inter-relation, see Figure 9.4.

5.1 Definition: What Makes Security Deviant?

The commission of crime and protection of crime and the criminal are not only inextricably linked from a criminological viewpoint, but also from a legal perspective. In short, criminal law defines the referent object whom conducts security deviant practices. How deviant security is further constructed and perceived in substantive and procedural law is shown by a brief analysis of two legal sources: i) national public law, more specifically Dutch substantive and procedural law, and ii) international public law, i.e., various conventions of the

Council of Europe that predominantly aim at harmonizing national procedural and substantive laws of states parties [82, p.215]. The last paragraph of this section concludes that the normative definition for deviant security is empirically observable. Security practices of cyber criminals may truly deviate from law-abiding entities which holds several consequences for researching DevSec.

Defined by criminal law In this study, the referent objects of security are cyber criminals. From a criminological perspective, these referent objects execute a modus operandi that consists of the commission of crime and the protection of crime and the criminal. In other words, commission and protection are inseparably entwined. Because of the legal connotations of the commission of crime, a definition for deviant security requires a legal approach as well. Irrespective of the legal system of jurisdictions [324], *who* and *what* are deemed criminal are legal constructs, and therefore must comply with the elements of criminal liability such as, but not limited to, the elements of *mens rea* (for elements in US law, see box Legal connotations to assets in Section 5.5) [325]. If these elements are proven beyond a reasonable doubt, an individual is criminally liable for the crimes he/she committed. This legal responsibility of an individual for the commission of crime is a *conditio sine qua non* for defining the referent object of deviant security. Thus, the latter part of an MO - i.e., the protection of crime and the criminal - is also understood from a legal perspective. Simply put, deviant security practices are the countermeasures of a legal or natural person who is criminally liable for the crimes he/she committed. This makes deviant security practices a legal construct and a normatively-laden concept as well. Therefore, this study subsequently defines deviant security as:

> all technical computer security controls of natural and legal persons who are criminally liable for the commission of crime, in order to protect the criminal and his/her crimes.

The next paragraphs continue by explaining how national and international public law - predominantly Dutch substantive and procedural laws and various conventions of the Council of Europe - further fine-tunes the definition for deviant security.

Constructed by absence of law Firstly, the definition for DevSec is further shaped by the *absence* of regulation. Besides a few exceptions (see Section 5.3), generally, neither the assets that DevSec has to protect, nor DevSec measures themselves are protected by private and public law. Similarly, neither are there any industry standards for the security of cyber criminals. The criminal assets that DevSec practices have to protect may also differ from bonafide assets of law-abiding citizens (see also Section 5.4). The latter are *defined* and *protected* by e.g., tax and intellectual property laws that do not apply to criminal products and services. Obfuscated malware cannot be regarded as intellectual property, neither can a cyber criminal get an insurance against rippers, nor put his/her fire arms on the balance for a tax refund. Basic civil law principles such as *pacta* *sunt servanda* - agreements must be kept - do not apply to the contracts between, let us say, a malicious crypter and his/her client. The only effective criminal contracts are indeed self-enforcing contracts as they lack third-party contractual enforcement [326, pp.26-27]. To induce a desired behavior, cyber criminals have no other option than offering carrots - rewards like the bug bounty program for cryptomarket members [327] - or hitting others with sticks, i.e., punishments like bans from fora as described in Section 6.6.

Law may also prescribe security standards to norm-addressees in order to protect computer users in general, but does not do so for law-breaking referent objects and/or any unmistakable deviant security mechanisms that protect criminals. For example, legal provisions such as the European Union 1999 eSignatures Directive dictates that qualified trust providers such as certificate authorities should provide trusted encrypted communications for computer users (see also [74]). There are no laws, however, that demand that criminal trust providers - i.e., escrow services - comply to a certain standard (see Section 6.4). This is one of the reasons why cryptocurrencies are popular among cyber criminals. The related cryptocurrency payment systems provide a level of deviant security because these decentralized systems lack legal and/or technical mechanisms that empower central authorities like mandatory authentication, payment processing based on intermediaries and the possibility to revoke transactions [328][329][330].

Constructed by procedural law The definition for DevSec is further finetuned by explanatory reports of procedural laws from, in this study, the Netherlands. In other words, do Dutch legislators identify and acknowledge the existence of deviant security practices as a problem for police investigations? Explanatory reports of the Dutch Code of Criminal Procedure (DCCP) explicitly mention administrative and physical (read: offline) DevSec practices of traditional criminals, and later in time, also online and technical security of cyber criminals. Of importance are the outcomes of the Dutch Parliamentary Inquiry Committee into Criminal Investigation Methods (1994-1996, see [331] for the reasons and findings of the committee). The committee provided the foundation for the procedural Act on Special Investigative Police Powers (*Bijzondere Opsporingsbevoegdheden*, also known as *BOB*), effective as from the year 2000. This act was specifically designed to regulate various intrusive investigative methods to fight organized crime. The research group of the parliamentary inquiry committee defined organized crime in 1995 as 'groups [...] capable of effectively shielding their activities against targeted actions of the government' [332, p.9]. The researchers distinguished between defensive and offensive contra-strategies, which is similar to terminology as active and passive disruption from more recent computer science research on botnet protection [158, p.129]. The defensive contra-strategies are ways of criminals to conceal their activities against competitors and government such as changing cars to thwart police observations. The offensive contra-strategies - very much the focus of the research group - are the willingness and ability of organized groups to actively fight government action [332, p.28], and include:

- The use of physical violence and intimidation;
- The elimination of individuals by way of corruption;
- The collection of information about government activities to subsequently adjust their own criminal activities (i.e., contra-observation);
- The use of media to create a favorable reputation or to discredit the government;
- The deployment of powerful and important individuals to influence government decisions;
- The distribution of disinformation to distract the government (e.g., double informants) [332, pp.133-134].

In fact, it is very much because of these deviant security practices that Dutch procedural law, i.e., Titel V of the DCCP, also allows investigations of those involved - i.e., *not* being suspects of crime yet - in planning to commit serious and organized crimes. According to the Dutch legislator [333], law-enforcement agencies need a proactive stance against these organized groups, and actively breach their deviant security to identify the offenses these criminal organizations are committing, as it is unlikely that (their) victims and witnesses will come forward and file a complaint.

How should we perceive the above mentioned DevSec practices from a technical computer security perspective? All measures are either *administrative* or *physical* countermeasures, of both *defensive* and *offensive* nature, against government action, see Table 5.1. Bribery as criminalized in the Council op Europe's Convention on Corruption is, for example, an administrative security measure, while the use of violence is a physical security measure. Defensive and offensive deviant security mechanisms of a technical nature, also deployed against other threat agents than the government, are not included in the report from 1995. Yet the explanatory memorandi of the Computer Crime Act III (*Wet Computercriminaliteit III*) in the Netherlands explicitly mentions breaching *technical* security of a *defensive* nature, like encryption, in a cyber criminal context [334, p.6]. Similarly, the explanatory report of the Convention on Cybercrime names encryption, intentional manipulation and deletion as means designed to destroy evidence [335, pp.3, 21]. Still, the fact that security practices may also include technical countermeasures of an *offensive* nature is *not* recognized as such in any of these explanatory reports.

The best defense is a good technical offense?
Cyber criminals do launch attacks for security purposes. The Rombertik malware conducted a DoS attack on forensic tools. It called the Windows API OutputDebugString function 335.000 times as an anti-debugging mechanism [336]. Cyber criminals also initiated major and persistent DDoS attacks against the website of the public-private No More Ransom initiative to prevent that their assets of decryption keys are distributed to their victims [337]. During this study, malware developers further put a threat into their ransomware code. In a line of code they stated that if the security researchers of a specific AV vendor would decompile their malware, they would publicly accuse the researchers of illegally hacking their servers. A last example of an attack for security purposes is the DarkSeoul malware that after successful installation on a victim's machine, disabled the main processes of legitimate antivirus software to avoid detection [338]. A last example is cyber criminals who discussed the idea of discrediting the work of a private security researcher. By adding legitimate websites in malware code, ISPs that used the researcher's botnet tracker would incorrectly label these sites as hostile, and hopefully stop using the tracker [339].

Moreover, the European Convention on Human Rights (ECHR), the DCCP and the Dutch Police Act (DPA) *implicitly* acknowledge that breaching DevSec is an inherent part of executing investigative powers. The DCCP and, when specific investigative powers are not codified in the DCCP, article 3 of the Dutch Police Act prescribe *what* the police is allowed to do, but *not* so much *how* the officers should execute investigative powers. Of course, these powers should be in accordance with article 8 ECHR (the right to private life and family life) and legal principles as subsidiarity and proportionality. For example, the DCCP prescribes that officers are allowed to conduct a house search (*what*), but does not expand on search methods and techniques (*how*). What if a door of the suspect's house is fortified? Here come article 7 of the Dutch Police Act and article 1 par. 3 sub b of the Police Instruction (*Ambtsinstructie*) to the rescue: officers are allowed to use all necessary violence to achieve their goal. This means that investigators may kick in a fortified door during a house raid. Still, articles 6:198 and 6:200 of the Dutch Civil Code (*Burgerlijk Wetboek* or BW) demand that the police adequately locks the kicked-in door after the search. In other words, the police must restore the suspect's security to a sufficient level against other threat agents after execution of its investigative powers. Similarly, the police is also allowed to brute force a seized but encrypted server, hack an electric door lock of a car to install an electronic listening device, and/or put some psychological pressure on a suspect during an interrogation. Law-enforcement agencies have no other option but to exploit these human and technical weaknesses. Without such legally allowed breaches, police investigations as truth-seeking processes would be pointless because collecting evidence is impossible.

DevSec found in procedural law	Defensive nature	Offensive nature
Technical security	✓	×
Administrative security	✓	✓
Physical security	✓	✓

Table 5.1: Legislators acknowledge most types of deviant security controls in explanatory reports of Dutch procedural law, with exception of offensive countermeasures of a technical nature like email floods.

Constructed by substantive law How does the criminalization of certain deviant security practices in substantive law further construct the legal definition for DevSec? Commonly, administrative, physical and technical countermeasures of an offensive nature are criminalized, see Table 5.2. Examples of such punishable acts include crimes against public authorities in general (articles 177 to 206 of the Dutch Penal Code (DPC) and the Criminal Law Convention on Corruption) like actively thwarting investigations and bribing judges; online and offline violent crimes against e.g., children (articles 239 to 254a DPC and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse); and various forms of unlawful interception of communications (articles 139a to 139f DPC and article 3 of the Convention on Cybercrime).

Is the same true for the criminalization of defensive acts of deviant security? There are few instances where the appliance of defensive administrative and physical security measures are criminalized in the Dutch Penal Code. Examples of the latter are offline means of money laundering like article 420quater DPC and article 6 of the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime that prohibit knowingly hiding, disguising and disposing financial objects that originate from crime. Hiding objects is known as security through obscurity: a security policy, yet a poor one [59, p.34]. Administrative deviant controls of a defensive nature include security through deception: deception tactics like administrative acts that help to avoid detection and discourage potential attackers, such as law-enforcement. Examples are forgery of documents, information and biometric characteristics (articles 225 to 235 DPC and articles 7 and 8 of the Convention on Cybercrime), e.g., using false passports/credentials.

However, no punishable acts of defensive technical security are found in the Dutch Penal Code and conventions of the Council of Europe, perhaps because these controls typically serve a dual-use purpose ‘that guarantee anonymity in legitimate actions [but also] provide new means to violate laws and hide the identities of lawbreakers’ [340, p.200]. These products can be used by law-abiding and law-breaking entities alike. So, proposals of law-enforcement, politicians and legislators to criminalize the intentional use of cryptography in the commission and concealment of crime would be a break away from current legal reality. Still, the US Committee to Study National Cryptography Policy already concluded in 1996 that two approaches could be taken to criminalize the use of cryptography for criminal purposes, namely as a blank provision or as an aggravating factor for a specific list of crimes. At the same time, the committee acknowledged that there are considerable interpretation problems with terms as intentional use and cryptography [341, pp.273-274].

DevSec found in substantive law	Defensive nature	Offensive nature
Technical security	✗	✓
Administrative security	✓	✓
Physical security	✓	✓

Table 5.2: The Dutch Penal Code does not criminalize the possession and/or usage of technical defensive DevSec controls with dual-use nature like secure-deletion software.

Empirically observable appearance & consequences Although DevSec is *defined* and constructed by formally enacted rules (read: criminal law), DevSec is further *shaped* by multiple forces. These forces include informal social norms enforced by potential threat agents other than LEA, such as individuals in the direct social surrounding of the cyber criminal. For example, a father approved of the cyber crimes that his sons were committing. As a result, they did not have to take any additional physical security measures to shield their crimes from their father at home. Chapter 7 gives an in-depth discussion how DevSec is further shaped by cultural, local/global, macro/microeconomical, political and technological dimensions.

Because of the real-world effects of (the absence of) law and other forces, the security of cyber criminals becomes *empirically observable* which holds several consequences for this study. Firstly, the appearance of DevSec practices may truly *deviate* from the security practices of law-abiding entities. Law-abiding entities do not intentionally host their legitimate content on the servers of bulletproof hosters, buy a VPN for a premium price on an access controlled cyber criminal forum, or take a subscription at a counter-AV services to test their software. Additionally, defensive technical deviant security controls are dual-use products, and not prohibited by substantive law, yet frequently misused by cyber criminals. Hence the semantic meaning of the word deviant which covers the legal and empirical reality of security by cyber criminals more appropriately than labels as criminal security or unlawful protection.

Secondly, the idea of empirically observable DevSec means that the security of cyber criminals becomes observable and measurable in respectively a *qualitative* and *quantitative* manner. Qualitatively, DevSec is *of a kind* and *to a degree*. An analogue example to explain this argument is a criminal who applies physical security to protect his/her home. He/she can choose from various kinds of locks, such as a cylinder lock on his/her door instead of an electronic lock. The degree of physical security may vary, depending on the situation. The cylinder lock might not be used when an individual feels safe in comparison to a situation where there is a high chance of theft by a ripper. Deviant security practices can also be converted to a *numeric* format and as such become quantifiable. We could measure the increase of technical security controls of a forum over time, the probability distribution of DNS fast flux of a botnet, or the correlation between the demand of a DevSec service and its price.

5.2 Meaning: Subjective Condition

As discussed in detail in Chapter 3, deviant security is perceived in this study as a *social practice* between a certain *us* and *them.* These practices are a continuing activity: security must endlessly be tested against known and hypothetical threats of a range of actors. These continuous threats to the security of cyber criminals has also resulted in a professional DevSec industry with DevSec practitioners, such as suppliers of bulletproof hosters and VPNs (see Chapter 6). This view sees security very much as *a means to an end.* However, Zedner argues that security from a good guy perspective can also be *a state of being* [106][31]. This section takes this position as a starting point to assess what the meaning is of deviant security, its state of being either as an objective or subjective condition.

Not an objective condition Firstly, DevSec as an *objective condition* implies a situation without any threats [106, p.155]. This presumes a world in which cyber criminals have no threat agents and can therefore freely commit crime. They are free from fear and do not need to apply any controls. In this utopian situation, cyber criminal do not require to be referent objects of deviant security. Of course, this condition does not match reality. In the real world, cyber criminals will *always* face a number of threat agents, threats and attacks. In fact, cyber criminals are continuously surrounded by enemies (see Chapter 6).

Could DevSec as an objective condition then be defined as a state of being protected from threats? Zedner names neutralization, avoidance and nonexposure as means for law-abiding entities to achieve this condition [106, p.155]. Indeed, we learn from this study that cyber criminals apply technical computer security to pursue this goal but never achieve it. Even if this objective state is attainable, new threat agents and/or threats could emerge. Thus what is secure today, might well be outdated tomorrow. Legislators might allow new investigative powers; a trusted co-conspirer might turn into a highly aggressive competitor in the underground economy; or AV vendors might find a way to prevent ransomware family from being profitable. These examples indeed prove that objective security is defined by reference to what is deemed a threat [31, p.15]. Moreover, the protection of crime and the criminal can never be 100% waterproof because deviant security is inextricably linked to the commission of crime. An aspect of this inseparable link is that cyber criminals face a tradeoff between *the commission of crime versus the protection of crime and the criminal.* This is essentially a *value tradeoff* as a suspect must make a judgement 'about how much [he/she] would give up on one objective to achieve specific amounts on other objectives' [342, p.935], with very successful criminals finding the perfect balance between both commission and protection instead of regarding security as an after thought. Cryptocurreny miners who deploy malware, for example, must balance the mining of potential revenues versus the risk of being detected by the true owner of the infected machine [184]. Cyber criminals may use legitimate freemium web analytics services to optimize their phishing sites, which turns out to be a vulnerability when the data that these services collect about the criminal and his/her crimes are shared with LEA or the private security industry. Another observed case includes 'sleeping' money mule accounts on an infected machine of a victim, waiting to be activated by the group behind the MYFL malware to transfer the stolen money, promoted the commission of crime. Once discovered by the banks, these accounts negatively affected the security of the mules. In other words, striving for perfect DevSec against threat agents and threats/attacks lays a heavy, if not unsurmountable, burden on the efficiency of the criminal business processes. Absolute deviant security against threat agents and threats actually leads to a paradoxical situation in which the cyber criminal has to pay the ultimate *opportunity cost* of not being able to commit any offenses. Lastly, objective security is unattainable for cyber criminals because components of the security cycle - threat agents, threats and valuables, including the referent object of DevSec (the criminal and his/her crimes) - are not set in stone but subjective and/or normative constructs that are subjected to changes in time and place. This argument is further elaborated on in the next paragraph.

To conclude, DevSec as an objective condition is out of reach for cyber criminals, and the cyber criminal community is well-aware of this issue. For that reason, cyber criminals may attend bonafide conferences on technical computer security, start threads with lively discussions about all sorts of security related topics on fora, and update dual-use security software on their machines to avoid exploitations of vulnerabilities by threat agents. Thus, the *material meaning* (see [106, p.160][31, p.21]) of deviant security lies in the empirically observable efforts of cyber criminals to invest in continuous learning about threat agents and threats/attacks, patch vulnerabilities, reduce risks, avoid damage to assets and install countermeasures.

Subjective condition DevSec is rather a *subjective condition*: the sense of cyber criminals about their own safety. In other words, this condition does not refer to any objective state, but only to the feelings of cyber criminals about their security. Still, these feelings may be correlated with objective conditions of security [106, p.156]. As described in the previous paragraph, components of the security cycle are subjective. There might well be a security gap between what the cyber criminal regards as a threat agent, threat/attack, vulnerability, risk, asset, risk or countermeasure, and how other key players (like LEA) interpret these components [106, p.156]. Such mismatches are essentially either vulnerabilities for cyber criminal, or missed investigative opportunities for law-enforcement agencies. At the same time, what is considered legal and/or an allowed practice by bonafide entities - e.g., ISPs that permit IP spoofing from their servers - might actually be a condition for cyber criminals to label that entity as being bulletproof against actions of key players from the cyber security community.

While research on deviant risk perceptions is absent, several cases are observed in which DevSec practices were virtually absent or very low. These instances provide evidence that at least some professional cyber criminals underestimate the risk on exposure. They might feel absolutely safe - a ‘qualified condition of freedom from anxiety or apprehension’ [31, p.16] - that leads to an *optimism bias*, read: underestimation of security risks. For example, an individual posted a video on social media, depicting himself while freely talking about the cyber crimes he committed. However, an investigative journalist discovered the clip and published an article about him [343]. Moreover, because of the decontextualized nature of the Internet [344], some individuals might not know that they have trespassed the law, and therefore apply little to no security. The very absence of any DevSec controls in an MO may be an indicator that there was no or little intent to commit a crime, and thus indeed be a legitimate defense and/or a reducing factor in sentencing [345]. The opposite idea - security may prove intent - is confirmed by Dutch court decisions in which the judges ruled that technical protective measures, more specifically encrypted and/or password protected folders containing CSAM, provides evidence that a suspect intentionally downloaded and stored illegal content [346][347]. Similarly, administrative security measures, such as appointing socially vulnerable straw men for business holdings, giving them nicknames while solely communicating through Tormail and taking their debit cards from them, proved that a financially-driven computer-focused criminal had knowledge about money laundering via his companies [348].

‘Let me help you with your security!’
During this study, an adolescent defaced the website of a small municipality in the Netherlands, and intentionally added information about his true offline identity. He placed a message to the website saying ‘Hi municipality [of town X]! Say hello to your colleague [very specific name Y] who is a friend of mine! Regards, [nickname Z]’. As it happened to be, Y was indeed working for municipality X, and knew defacer Z. Just a single phone call to the town hall was needed to solve the case, and Z accepted a transaction of the Dutch Public Prosecution Service to do 40 hours of community service. *Responsible disclosure policies* of several hardware manufacturers, like [349], prescribe that vulnerability reporters must announce their organization and name. This ensures that reporters give up the security that protects their identity and, as such, show their good intentions. A situation has been observed in which unknown individuals who obscured their true identity kindly, but persistently, demanded a ‘reporter’s fee’ in cryptocurrencies from a business for finding a vulnerability in the company’s system that hold sensitive personal and company data. They further stated that ‘it is a pity if somebody would post the data publicly’. The combination of financial demands, warnings about possible damages and deviant security measures alerted the company that these individuals might not want to comply to the installed responsible disclosure guidelines, and was subsequently the reason for the company to inform the police about a possible extortion. These examples and the previously mentioned court cases show that deviant security is used by the judiciary as an indicator of intent that could be established according to objective standards, read: common and custom rules and factual circumstances, while personal characteristics - thus a more subjective approach - may also play a role like personal knowledge and previous experiences [350, pp.187, 211].

In this sense, the *symbolic meaning* of deviant security - i.e., the assurance that 'something' is done against threats - addresses these subjective feelings. The symbolic role of security to cyber criminals seems ambiguous. Besides persistent spam messages and advertisement banners [229, pp.40-41], few rhetoric and strong emotional appeals by DevSec providers on fora have been observed during this study, such as aggressive marketing and sales strategies in which they overreact for inflated threats agents and attacks. Forum discussions about security, especially vulnerabilities, are usually on-topic and realistic, while threads and posts are of members who have no other interest than avoid getting caught. Moreover, evidence from investigations shows that some bulletproof hosters (BPHs) give surprisingly little assurance to their customers about their ability to protect them.

On the other hand, cyber criminals might sit in a *security theater*: a situation in which countermeasures merely provide the feeling of security while doing little to nothing to achieve it [351][31, pp.21-24]. For instance, providers of deviant security - like bulletproof hosters - have been observed during this study who assured clients about their capabilities to protect them from law-enforcement agencies. In reality, their statements were make-belief promises as these facilitators were subjected to police investigations at the time. The investigators discovered that these cyber-crime-as-a-service providers had not installed some of the most basic technical computer security controls to protect e.g., their customers. Likewise, DevSec measures may also merely meet concerns about *subjective insecurity*, but not about the actual threat. Small fortifications will not delay the police from entering a building or room, but rather result in the deployment of special weapons and tactics units (commonly referred to as SWAT units) and use of excessive force (also known as no-knock warrants).

5.3 Provision: Club, Common, Private and Public Good

After the definition and meaning of deviant security, this section describes and explains how DevSec is supplied to referent objects. Like good guy security [352][353][354], DevSec can be provided as a club, common, private and public good, distributed in either a centralized or decentralized manner. Two characteristics are vital to distinguish and understand goods. *Rivalry* means that a good can not be used by two individuals at the same time. *Excludability* means that an individual has exclusive control over a good and that others are excluded to use that good [352, p.78][355, p.11], see Table 5.3.

Private good: excludable and rivalrous Deviant security controls can be a private good, thus excludable and rivalrous. This becomes apparent in the commercial and proprietary nature of some of the observed cyber criminals' countermeasures. Cyber criminals purchase dual-use intangible security software of bonafide companies to protect their systems and data [356, p.15].

Forum administrators deploy commercial DDoS mitigation services of legitimate technology companies to provide system *reliability* - i.e., continuity of correct service [66, p.6] - of their online market places, and thus ensure availability of their platform to forum members [53, p.549]. Malware developers and crypters may test their obfuscated malware against legitimate antivirus products via counter antivirus services (CAV, see Section 6.6). Similarly, legitimate programs might protect botnet panels against brute force attacks and SQL injects. Dual-use purpose countermeasures also include tangible products sold in spy shops, such as recorders, cell phone scramblers, global positioning system (GPS) jammers, or hidden compartments and pointed weapons in, for example, flash lights. Of course, not all commercial security is legitimate and/or serve a dual-use purpose. There is also a vivid underground economy where cyber criminals can buy a range of specialized deviant countermeasures, i.e., *deviant-security-as-a-service*. In these cases, individuals pay others for their DevSec, and in turn receive security products and services such as bulletproof hosting, malware crypting or money laundering. Those who are not part of the transaction, have no control over these DevSec controls, and as a result, cannot consume them at the same time.

Club good: excludable but non-rivalrous Deviant security can also be a club good, so excludable but non-rivalrous. Members on closed cyber criminal fora and of organized groups have their own individual *deviant security interests* that are partly conflicting and partly matching the interests of other members. They aim at *multilateral security* [64, p.49]. Security conflicts are recognized and compromises negotiated, mostly via long group discussions and/or direct interventions of forum administrators (also known as admins). Moreover, community members helps each other out to keep the individual's and group's security up-to-date, without outsiders profiting from these provisions. In such access controlled communities, security is very much a peer-produced good. This good does not only include sharing administrative security policies (rules, news and so-called tips & tricks), but also technical security controls. Most fora have threads where members post - amongst other things - license keys of bonafide antivirus software that other members may use for their own benefit. The latter is an example in which security is completely decentralized by its members. Yet forum administrators formulate policies and implement countermeasures as well, and as such ensure that security as a club good is also provided in a more centralized manner to its associates. Throughout this study, examples are given of systems of cyber criminals, such as cryptomarkets and fora, with *incentive centered designs* (ICD) that focus on 'getting the good stuff in and keeping the bad stuff out'. These designs respect motivated security behavior of individuals by providing incentives to induce human choices that improve the effectiveness of the system's security at large [357, p.7].

Public good: non-excludable and non-rivalry In DevSec as a public good, there is no rivalry and no excludability for the referent objects. Firstly, security is provided by free and/or open-source security products in a decentralized manner. Collective goods include the criminal usage of free, automated and open SSL/TLS certificates; open-source challenge-response tests - i.e., captchas - to protect fora against brute force attacks; the usage of free public Wifi to surf on the Internet [320, p.10]; or freely available artefact wiping tools for the purpose of data sanitization. In these instances, deviant security is a peer-produced public good provided by civil society, like individual netizens, online communities, and private and public organizations. No matter if entities are trespassing or abiding the law, they will all receive the same kind and degree of security.

Centralized means of control, like national laws and government policy, may also provide security as a public good to cyber criminals. Apart from justifiable acts (also known as justification), unlawful acts by threat agents against the security of criminals are very much violations of substantive law as well, and punishable as such. This might result in exclusion of evidence from such breaches in court, and deter other threat actors to attack DevSec at all. Law may also protect criminals against specific attacks under all circumstances. The protection of the physical and psychological integrity of the criminal is fundamental in most international and national public legal frameworks. The absolute prohibition on torture (article 3 ECHR) and the right to remain silent (*nemo tenetur* - included in article 6 ECHR) protect suspects against disproportional government actions. There might also be active government policies to protect cyber criminal practices. In response to the arrest and extradition of Russian suspects from various (holiday) destinations to the United States [358], Russia issued travel advisories for their citizens in 2013 which countries are considered 'unsafe' [359]. Additionally, there are not only continuous rumors in news media outlets but evidence is also brought forward by the US Department of Justice about Russian criminal hackers that are protected and even deployed by Russian authorities [360][361][362].

Common good: rivalry but non-excludable Lastly, DevSec can be rivalrous and non-excludable, namely a common good. Today's cyber crime is organized in networks, especially due to the emergence of cyber-crime-as-a-service. For all actors in these networks, deviant security is very much a common good which everybody needs. However, because actors have different perceptions on-, motivations for-, and interests in deviant security, they may also consume each other's security instead of promoting it, thus effectively lowering the security of all. Let us take the so-called pharma wars as an example: a turf war between two sponsors of pharmaceutical spam as described in the non-fiction book Spam Nation by investigative journalist Brian Krebs [211]. The pharma wars were in essence a *competitive escalation* that led to a *destructive conflict* [363, pp.241-242]. The same line of reasoning goes for cooperative suspects and criminal informants who share information about their colleagues with LEA. By breaking their silence (*omertà* [364, p.6], or external secrecy), they effectively lower the security of their co-conspirers which causes a classic *prisoner's dilemma.* In other words, they may make decisions that benefit their own security, but negatively affect the overall security of the larger cyber criminal collective. So, not only the security of law-abiding entities [352], or the commission of cyber crime - like phishing attacks [365] - are *limited resource economies*, but the deviant security of the cyber criminals as well.

Provision of DevSec goods	Excludability	Non-excludability
Rivalry	Private good: commercial dual-use security products and tailor-made DevSec services	Common good: controls that will increase an individual's security at the expense of the security of the larger cyber criminal community
Non-rivalry	Club good: peer-produced security within closed cyber criminal groups	Public good: free & open-source security products, and active government policies & absolute human rights

Table 5.3: Excludability and rivalry are key to understand how DevSec can be provided as a club, common, private and public good.

5.4 Function: An Asset To Protect Assets

In the Information Age, everything that relates to information technologies (IT) - i.e., data, software and hardware - has extreme value to both law-abiding entities and criminals alike (in other words, become *assets*) [28]. While assets are important in a range of academic disciplines including computer science, no studies are found that provide a taxonomy for assets of cyber criminals. This section first determines what cyber criminal assets are from a predominantly socio-legal perspective. Such an understanding not only helps to determine which valuables need security (for a summary, see Table 5.5), but also what deviant security is in itself: an asset that protects assets.

Assets relate to the criminal and his/her crimes Assets of cyber criminals relate to the two key components of an MO, more specifically i) the criminal and ii) his/her crimes, the latter consisting of both his/her conduct and the outcomes of his/her conduct. As compared to the latter assets, valuables related to the criminal are - or ought to be - more important, at least from the perspective of law-enforcement agencies [206]. Any damage against these assets may ultimately result in violations against the suspect's physical and/or psychological integrity. So identity assets are not only beneficial for commission, but also protection. Sharing personal details can, for example, be an important factor for building trust among (potential) transaction partners, including having a reputation of being trustworthy [115]. Similarly, protecting identifiable details is also important to suspects of crime because the exchange of personal information may hold blowback effects such as identification by threat agents. Loss of, or damage to, identity then comes at great costs like arrest and prosecution that will ultimately also harm the commission of crime. The formidable reputation of Russian cyber criminal Paunch in the underground economy was important to attract other skilled co-conspirers and customers to the Darkode forum [366], but at the same time, half of the international LEA community was trying to compromise his identity assets for attribution purposes (i.e., who did what).

The second asset category relates to criminal activities. These assets have, according to the motivation for crime, financial, political, sexual and thrill-seeking value. In practice, a criminal may attribute multiple values to an asset. A data asset such as a carefully collected CSAM series does not only have sexual, but also financial and emotional value, respectively when CSAM is sold via a commercial website, or contains identifying details of the perpetrator and/or victim. The value of assets may differ. Complete credit card credentials - 'fullz' - are more expensive than partial information such as 'dumps' and 'CCV2' [320, pp.3-4]; new CSAM is more in demand than old, 'recycled' material; zero-day exploits are preferred over well-documented exploits; and early issued ICQ numbers - an instant messaging client popular among Russian-language cyber criminals [367] - help to boost reputation as these numbers imply a long presence in the underground economy and are therefore more exclusive than recent ICQ numbers.

Protection of the criminal versus his/her crimes
Cyber criminals may face a *zero-sum tradeoff* between securing assets related to criminal versus his/her crimes. Indeed, it is easy to theorize that the protection of the cyber criminal should always prevail over the protection of crime. Harm to the criminal - like arrest and prosecution - has the potential to stop all business proceedings on a more permanent basis. However, cyber criminal may also choose for the protection of crime instead of the criminal. Several cases have been observed in which profit-driven cyber criminals used their true credentials to register an account of an underground and/or legitimate bank that holds their illegally obtained gains. The underlying thought is probably that they were afraid that they would lose their financial assets when they cannot prove to the financial service provider that the subscriber details match their real offline identity. After all, they are in to this business for the money.

These two asset categories may collide as cyber criminals frequently need identification to achieve *integrity, availability* and *confidentiality* for the protection of their business and, paradoxically, their identity as well. Cyber criminal fora may deploy access control management to offer a safe business environment for their members. The forum members need to be identified with the use of a username, email address or account number, and authenticated using a password in order to be authorized to access data and to be hold accountable for actions. Nota bene, verification links might be send to chat and email services, while disposable temporary email accounts are not allowed for that purpose [368, p.6]. Due to such strict access controls, forum members face for a dilemma. This security mechanism is needed to protect the criminal and his/her crimes, but in order to do so they have to reveal clues about their identity. This poses a risk, especially when authentication mechanisms are badly implemented and exploitable with brute force or dictionary attacks [155]. Not only can hackers use login names, email addresses and passwords to take over the accounts of forum members, but this data are also important leads for attribution by law-enforcement agencies. So, access control causes a paradoxical situation: cyber criminals need security to protect their identity and business, but in order to do so they may have to violate their privacy.

Tangible assets A further categorization can be made between tangible and intangible assets. Assets of cyber criminals, as described in Section 5.1, differ from bonafide assets as only the latter can be legally protected by e.g., binding contracts and patents [369]. Therefore, strict implementation of asset categorizations from the good guys perspective is impossible. Still, widely accepted asset categorizations - e.g., the Balanced Scorecard [370][371] - combined with criminal and case law are a helpful starting point for understanding what cyber criminals and legal practitioners consider as criminal valuables. Although one might associate the practices of cyber criminals solely with the intangible online world, physical subjects and objects are also very important to cyber criminals and public and private cyber crime investigators alike [372]: all cyber-attacks stem from a person who physically exists in a certain location [364, p.1]. This study therefore distinguishes *tangible assets* for cyber criminals between:

– *Physical subjects*: human beings such as referent objects, clients, corrupt officials, co-conspirers, (criminal) informants, actual and potential victims, and witnesses (also known as the human factor in cyber crime and cyber security [215, p.15]). Dutch procedural law prescribes that police investigations must work towards the prosecution of suspects (articles 27 and 132a DCCP) and witnesses are obliged to give testimony in court (article 213 DCCP), while helping victims of crime is a key task of the Dutch police according to article 3 of the Police Act 2012 (*Politiewet 2012*);

– *Physical objects*, and more specifically:

  ◦ *IT focused physical objects*: IT objects are important because they consist of the hardware that is vital to commit cyber crime and in which digital evidence resides. Hardware includes computers (tablets, desktops, laptops, routers, servers and associated accessories like keyboards and monitors), telecommunications (cell phones and batteries, SIM cards, mobile WIFI) and other data carriers (USB sticks, SD cards, external hard drives). IT focused physical objects are not only central in the execution of a range of digital investigative powers and subsequent collection of metadata and content (read: evidence, see Table 5.4). They have also been the focal point of legal discussions about new investigative powers in cyberspace [373][374][375][21];

  ◦ *Non-IT focused physical objects*: administrative paperwork, buildings, cars, cash money, luxury items, payment cards and the like. These objects are often overlooked by academics in discussions about cyber crime, but very important to legal practitioners in investigations. Ultimately, cyber criminals use offices from which they commit their crimes, drive cars to meet other co-conspirers, and monetize their virtual dirty money in hard cash or luxury items [212][376]. Many traditional investigative powers focus on these non-IT objects, such as the recording of confidential communication in cars (known as bugging), confiscation of illegally obtained assets, or no-knock warrants to enter properties. These powers are frequently deployed in cyber crime investigations; if not *always* when investigations lead to physical arrests of suspects (see Table 5.4).

Although not fully exploited in Dutch cyber crime investigations [377], both non-IT as well as IT focused objects may contain forensic evidence like blood, scent and DNA traces and finger and foot prints. This physical evidence may help to attribute physical subjects to physical objects, and confirm or reject hypotheses such as ‘only suspect A’s DNA [Deoxyribonucleic acid] and finger prints are found on keyboard B and computer C. Therefore, it is highly likely that suspect A is the user of keyboard B and computer C’.

Seized physical objects in eight investigations	Number	%		*Number*	*%*
Non-IT focused physical objects	464	33			
IT focused physical objects	962	67	*Computers*	*130*	*14*
			Telecommunications	*389*	*40*
			Other data carriers	*443*	*46*
	1637	**100**	**Total**	***962***	***100***

Table 5.4: A total of 1637 objects were seized in eight investigations of the Dutch National High Tech Crime Unit (NHTCU). Bearing in mind that the NHTCU conducts large-scale operations against organized criminal groups, two investigations had over 450 seized objects, five investigations had between 450 and 100 seized objects, and in one investigation less than 100 objects were seized [377].

Intangible assets While this study considers tangibles as physical assets, intangibles are all non-physical assets. *Intangible assets* - also known as intellectual capital [378, pp.371-374][370, pp.20, 22] - can be distinguished between:

- *Human capital* (also referred to as knowledge assets [379]): the knowledge, experience and competencies that individuals need to commit crime including creativity, received training, reputation and talent.
- *Information capital*: the software and data in databases, information systems and technological infrastructures that cyber criminals need to commit their crimes, such as chat clients, malware, operating systems and stolen documents;

- *Organization capital*: the organized group's or larger community's culture, business processes and relations, its leadership, management and structure, alignment of its members with its strategic goals, and the community's ability to collaborate and share knowledge, necessary to commit their crimes.

Intangible asset categorizations to understand cyber criminal fora
The distinction between information, human and organization capital on both the commission of crime and the protection of crime and the criminal is most apparent on cyber-crime-as-a-service fora. Some members of these online platforms - so called leaders and motivators [380] - provide vital human capital (i.e., knowledge) about commission and protection to other members, including 'chatters', via threads and posts. The vendors on CaaS fora offer products and services - mostly information capital - that facilitate commission and protection like infected hosts, stolen credit card details or botnet panels (see Figure 6.2). Lastly, there is a small group of forum members that provides the necessary organization capital to keep the forum up-and-running, including arranging deviant security as a club good against inside and outside threats. Their formal status is simply known as administrators or admins, yet they have to make crucial security-related decisions about the forum. They perform roles and tasks equal to chief executive officer (indeed, somebody has to supervise daily business operations) and chief financial officer (for processing incomes from advertisements, fines and restitutions, and expenses like salaries, hosting and security). Admins also have to patch vulnerabilities, come up with deviant security policies and mechanisms, and resolve disputes. These jobs are comparable to respectively chief information officer, chief security officer, and chief legal officer. The latter functions as a *trias politicus* as there is no separation of powers on fora. Administrators and their helpers are often legislator, judge and executive in one.

Intangible assets generally do not create value on their own, and need to be combined with other intangible and tangible assets [370, p.21]. Developing and operating information capital like malware and botnets require human capital. If developed or operated in a group, organization capital is also needed. Similar to traditional criminals [198, p.202], organized business processes of cyber criminals require coordinated efforts over time as well.

Moreover, Dutch criminal law considers tangible assets as goods that represent financial value, but is ambiguous in regarding intangible assets as such [82]. Yet, similar to their bonafide counterparts [381], malafide intangibles may become tangibles when they are brought to the market and become part of a transaction, and as such are converted into monetary value. The importance of hard cash to cyber criminals - and broader: the idea of attackers as resource-limited actors [382] - becomes especially apparent in the communications between two individuals. They agreed that they had the human and organization capital to commit crime: they were very focused and had great ideas, technical skills and the network to make things work. They missed, however, the necessary money to buy the required information capital in the underground economy, such as malware components and infected hosts, and physical objects on legitimate markets like hardware. As a consequence, they concluded that were not able to conduct any illegal activities. Similarly, large amounts of hard currencies and luxury items are frequently discovered and seized during house searches such as two million Euro and thirteen (luxury) cars found on eleven premises related to a Dutch vendor of bulletproof telecommunications [383].

Assets that need protection	**Asset category**	**The cyber criminal**	**Sexually-driven computer-assisted crimes**	**Profit-driven computer-focused crimes**
Tangible assets	Physical subjects	The criminal him/herself	Child victims	Co-conspiring inject writer
	Physical objects: non-IT focused	(Copy of) passport	Printed photos of the neighbor's children glued to real-size dolls	Hard cash
	Physical objects: IT focused	Personal computers	Servers	Infected computers of victims
Intangible assets	Organization capital	Leadership; large supportive cyber criminal network	Culture of sharing abusive material on a forum; collaborations between CSAM producers	Organizational alignment to other services in the cyber criminal value chain
	Human capital	Status and reputation in the cyber criminal community	Grooming skills; finding and gaining access to exclusive online CSAM environments and images [384]	Hacking and/or malware writing skills
	Information capital	Unique pseudonym (i.e., nickname)	Child abusive images [385]; social media account with many befriended children	Virtual and cryptocurrencies

Table 5.5: Examples of observed assets, and their value to the criminal or his/her crimes. Because this study focuses primarily on cyber crimes for financial and sexual gain, assets with political and thrill-seeking value are not included.

Deviant security: an asset to protect assets The previous paragraphs discuss assets that are necessary for the commission of crime. These assets need protection because of the value that they represent for the well-being of the criminal and his/her business. Therefore, the commission and protection of cyber crime are inextricably linked to such an extent that it is hard to find instances where there is absolutely no security prior, during or after the commission of cyber crime. In a world of continuous online and offline threats, in which deviant security is in most instances not a publicly available good, security is very much an *asset* to cyber criminals, i.e., a scarce commodity in what sociologists David Lyon and David Wall name an electronic panopticon [386][34] (see Section 7.1). This is shown by the vivid underground market for a large variety of deviant security services. For instance, the services and products of bulletproof hosting and connectivity providers consist of - amongst others - anti-DDoS protection, dedicated/shared/virtual private servers, domain registration/protection, (double) fast flux, IP masking/spoofing, proxy servers, remote desktop protocol (RDP), secure sockets layer (SSL), Socket Secure protocol (SOCKS) and virtual private networks (VPNs) [255, p.31][387, pp.3-4]. Some of these protective services/products, like VPNs, represent *fixed costs* which do not vary with changing output. Whether a cyber criminal increases or decreases his/her commission, he/she only needs a single VPN subscription to safely access the Internet and therefore his/her monthly VPN costs stay the same. Other services and products related to bulletproof hosting and connectivity are *variable costs* to referent objects, and depend on changing output. If a suspect would like to increase the number of attacks, he/she might need more bulletproof servers, DDoS protection, domain registrations and the like. The subsequent prices of these deviant security assets are determined by - amongst other things - their quality and level of protection [388, p.10][267, p.171]. For instance, low-quality fake IDs are cheaper than high-quality ones. Moreover, DevSec products and services - like the mentioned hosting and connectivity services - are sold for considerably higher prices than comparable goods available on the bonafide market [256], sometimes, as observed during this study, up to ten times. Because the commission of crime differs among different types of cyber criminals, (the usage of) related protective assets do too. As compared to sexually-driven cyber criminals, profit-driven cyber criminals have to invest in additional security services like escrow services and cryptocurrency tumblers. Thus, the *total costs* (i.e., fixed plus variable costs) of deviant security are very much determined by the type of crime and criminal.

The criminal's perceived value of assets that are needed for the commission of crime can be measured by its level of security. Let us take spam servers and CSAM as examples. Spam servers generally rely on few, if any post-activity controls. The related IPs and domains are easily blocked and/or taken down by the cyber security community after usage as compared to C&C servers where criminals need availability of their servers, and therefore need additional tailor-made DevSec services to deal with incoming abuse notifications. The reason for little security is that when the spam run has been conducted, continuity is not required and therefore their job is done. In other words, the servers do not represent any value any longer [213, pp.176-177]. New - read: exclusive - CSAM is shared in highly secure environments, while older material is more accessible and found on open parts of the Internet [389, p.15]. There are also instances in which hardware, software, data and physical objects lack any security, and therefore appear to have no value to the criminal. However, the value of an asset is not only determined by its *objective value* (based on a e.g., monetary expression) and *subjective value* (based on e.g., symbolic, moral or emotional effects) to the referent object, but also by the objective (read: legal) value to his/her threat agents. Law-enforcement agencies may regard certain objects as assets because of their importance to police investigations. A CSAM user protected his home IP address with a VPN connection while downloading encrypted abusive material. The criminal did not place the same importance on protecting his home IP address when accessing another site which only contained the decryption keys as this act is indeed not an criminal offense on its own. The legal practitioners considered the connections to this decryption site as an asset for their investigation. They were subsequently able to retrieve the suspect's home IP address through lawful intercept. To conclude, criminal assets are not only valuables that generate and/or facilitate, but also *secure* the criminal and the commission of crime.

5.5 Form: Intangible and Tangible Products & Services

As we know what is the function of deviant security - an asset to protect assets - we move forward and describe in socio-technical terms what *form* deviant security takes, namely tangible or intangible, and as a dual-use product or as a tailor-made service. Table 5.6 is a summary and Figure 5.2 a visualization, of both intangible and tangible protective asset categorizations with related examples.

Intangible protective assets Similar to legitimate assets and assets related to the commission of crime, intangible deviant security assets can be categorized as human, information and organization capital. Because human and organization capital are very much soft controls - in other words, management-oriented - they are classified as administrative controls [59, p.28]. On the other hand, information capital on DevSec is categorized in this study as either administrative or technical controls.

– *Human capital* on DevSec consists of the knowledge, experience and competencies that individuals need to formulate deviant security policies, and to correctly implement these policies in order to protect the criminal and his/her crimes, including creativity, received training and talent. Observed knowledge assets are the many and constantly updated threads about security-related issues, including complete 'how-to-securely-commit-crime' manuals, on financially-driven cyber criminal and sexually-driven CSAM fora [320, pp.9-11][390]. Because technical deviant security constantly evolves, some threads about e.g., vulnerabilities in encryption standards on well-managed fora are more than ten years active, and continuously updated with the latest news and insights. Observed vulnerabilities of protective human capital include little understanding of technical computer security and *illusion of control biases.*

Previous experiences with the right to talk and/or remain silent
A suspect was arrested by law-enforcement and interrogated about the crimes he had committed. He was a first time offender, and therefore had no prior experience how to approach such an important event in the post-activity phase of his (ultimately unsuccessful) MO. The investigators later stated that they noticed his inexperience. Compared to seasoned reoffending suspects, he was both talking and remaining silent on the 'wrong' moments during the interrogation which was beneficial in building a criminal case against him.

- *Organization capital* follows the same line of reasoning. Cyber criminals are depending on co-conspirers in an ascending order of organizational sophistication: from colleagues, peers and teams to formal organizations [197, pp.157-158]. Alignment, culture, leadership, processes, teamwork and other capabilities of organizations are therefore not only needed to commit cyber crime, but also to protect the collective, individual members and their activities. According to private security researchers, organization capital was exactly why the Ponmocup botnet stayed under the radar for over ten years [391]. Observed vulnerabilities of protective organizational capital include little authority by group leaders, no internal rules or frequent violations of rules, and the inability to resolve conflicts.

- *Information capital* include administrative acts like legal registrations for protective purposes in e.g., offshore jurisdictions, legal immunities that prevent prosecution, or false credentials/records/subscriber information. They also consist of technical controls, more specifically intangible information technologies - i.e., software and data - such as tailor-made DevSec services (e.g., malware packers) and dual-use software products like encryption, firewalls, IDs and technical access controls. Observed administrative vulnerabilities include the blocking of financial accounts that were registered with false credentials, while technical vulnerabilities are of course identical to weaknesses of legitimate software (thus from a good guy perspective on technical computer security).

Notably, intangible protective assets may hold monetary value in the cyber criminal community. Deviant security consultants and technicians who advertise on cyber criminal fora and/or work within closed organized groups, see Table 6.2, sell nothing but human capital. They exchange knowledge about DevSec for money, and as such, convert the intangible to a tangible.

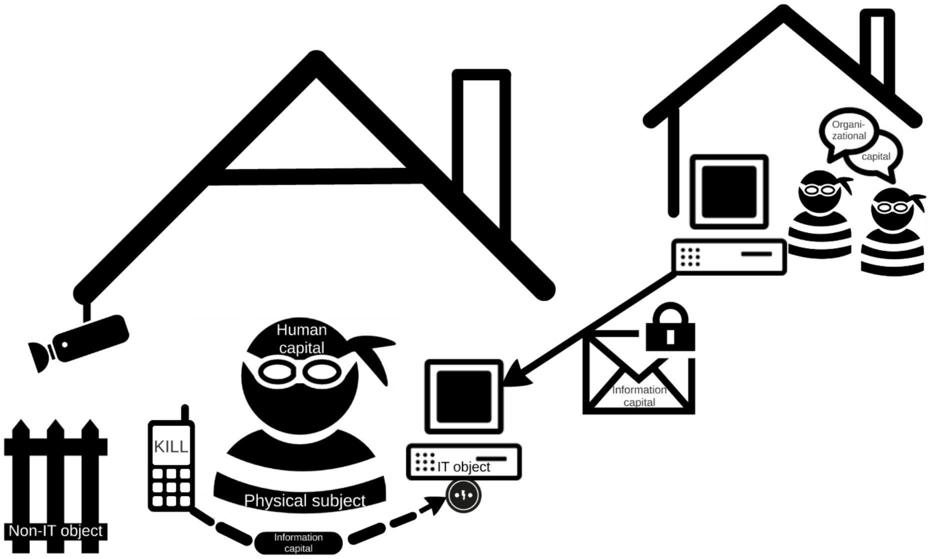


Figure 5.2: This picture shows various intangible and tangible assets that are needed for the commission of crime and the protection of crime and the criminal. Operation rooms, fences and CCTV are non-IT focused physical objects. A referent object - read: physical subject - needs human capital to understand how to operate a kill switch. The kill switch message itself is information capital while the sending and receiving hardware, respectively a cell phone and desktop, are IT focused physical objects. For successful collaborations, suspects need organization capital. They might agree that all communications must be encrypted. The encrypted messages between communication systems are considered information capital as well.

Tangible protective assets Tangible protective assets are all *physical* security controls, either subjects or objects, that protect tangible and intangible assets, including other deviant security assets. Tangible protective assets are synonymous for *physical deviant security*, and are discussed in-depth in Section 7.4. Again, tangible security assets are categorized as:

– *Physical subjects* who have a role in deviant security practices. Cyber criminals and other key players that are described in Chapter 6 conduct physical behavior that protects the criminal and his/her crimes. In other words, referent objects perform physical acts to install and maintain online and offline deviant security controls to protect themselves and other subjects - like their co-conspirers and victims - as well as physical objects. Observed human vulnerabilities include personality characteristics like laziness, forgetfulness, overconfidence and the propensity to engage in risky behavior [110, pp.1257-1258][292], and health issues such as mental and physical disorders - e.g., states of high sexual arousal - that promote accidents, failures and mistakes.

- *Physical objects* may also deliver security to the cyber criminal and his/her crimes, and is further specified as:
    - ○ *IT focused physical objects* are all hardware products that protect the criminal and his/her crimes such as physical access control, prepaid telephones, secluded business enterprise servers, routers with state-of-art encryption, and closed-circuit television (CCTV). As virtually all security IT focused physical objects come from bonafide vendors (see next paragraph), observed vulnerabilities are published and unpublished weaknesses in legitimate hardware. Notably, law-enforcement agencies can physically seize these objects, and as such, have the technical ability and legal mandate to exploit these vulnerabilities.
    - ○ *Non-IT focused physical objects* consist of fake passports, keys, locks and vaults, armored doors, weapons, fences, hidden passages/spaces, and even squeaky stairs that warn the cyber criminal about threat agents who are approaching his/her operation room. Observed vulnerabilities of non-IT focused physical objects include fake IDs with evidently false credentials, and cash money in hidden passages that were found by a trained police dog (also known as K9).

The municipality of Limburg
A non-Dutch suspect of online banking fraud purchased a fake Dutch passport in the underground economy to open a bank account in the Netherlands. The passport was apparently signed by the 'major of the Limburg municipality'. This alarmed a bank employee: while Dutch passports are indeed issued by local municipalities, Limburg is not a municipality. It is the name of two provinces in both the Netherlands and neighboring Belgium. In this situation, the suspect had too little human capital to assess the quality of his fake ID. In another reviewed case, a cyber criminal group behind a mobile banking trojan launched a landing page for phishing purposes. While the word login was spelled correctly in Dutch, the cyber criminals misspelled the word password (*wachtwoord*) in such a way that few potential Dutch-language victims would fall for the scheme.

Duals-use security products & specialized DevSec services So far, this study uses the terms DevSec products and services as if there is no difference between the two descriptions. However, there are specialized, mostly proprietary products for the commission of crime. These products, such as intangible malware and tangible skimming devices for banking fraud, are tailored to the needs of cyber criminals. Comparably, there are no DevSec *products* on the underground market that are specifically designed and manufactured for cyber criminals besides GPS and cell phone jammers. All observed security mechanisms which are used for DevSec purposes are dual-use products of bonafide entities, such as commercial parties or open-source communities. Examples are intangibles like encryption, obfuscation, steganography, cryptocurrencies; and tangibles such as encrypted phones with IMSI catching detection, firearms,

Protective assets	Security category	Asset category	Protecting the cyber criminal	Protecting sexually-driven cyber crimes	Protecting profit-driven cyber crimes
Tangible	Physical	Subjects	Flee and/or hide from LEA	Psychological violence against victims	Money mules & money mule handler
		Objects: non-IT focused	Fake ID	Closed curtains, soundproof rooms in remote area	Vault
		Objects: IT focused	Encrypted phone with privately owned business enterprise server	Power plug kill switch	Proxy server
Intangible	Administrative	Organization capital	Culture of not doxing or leaking	Sharing security manuals on CSAM forum	Authority and respect to avoid ripping by criminal partners
		Human capital	Discipline to withhold personal details	Deception skills (grooming)	Ability to choose identity over financial assets
		Information capital	Diplomatic immunity	Certificate of (good) Conduct	Offshore legal entity
	Technical		Obfuscated malware	Encrypted images	Cryptocurrencies

Table 5.6: Examples of observed assets and their value to the criminal or his/her crimes in socio-technical terms. Because this study focuses primarily on cyber crimes for financial and sexual gain, assets that need protection because of political and/or thrill-seeking motives are not included.

vaults and so on. All these products - again, with the exception of GPS and cell phone jammers - are legitimate (but sometimes licensed), widely available on the bonafide market, and neutral in the sense that the referent object of the security product decides whether they will be used to protect good or bad acts.

Legal connotations to assets
Criminal assets are not only combined by cyber criminals to create value, but also by legal practitioners to constitute criminal liability [298, p.1221]. Four elements are necessary for criminal liability under US law [392, pp.52-53][325]. Firstly, human capital connects to the mental element of crime, *mens rea*, and its subclass of criminal intent: knowledge of wrongdoing. Secondly, information capital and tangible assets connect to *attendant circumstances*, such as child sexual abusive material, malware on systems, and/or a victim. Thirdly, *actus reus* - the criminal's conduct - subsequently glues human capital to information capital and tangible assets, thus knowingly and without justification possessing, viewing, producing or distributing child abusive material. The last element is that there should be a *forbidden result* or *harm*, thus damage to assets, mostly related to victims like children who are physically and emotionally harmed for the production of CSAM. So, the involvement of assets described in this section - whether used for commission or protection - combined with the element of harm very much make individuals criminally liable, and further make that these assets differ from assets used by law-abiding entities. What about organization capital? This intangible asset is about the coordination between, and degree of involvement of, individuals in crime and their subsequent legal role as accomplices, accessories, aiders, abettors or conspirators as concluded by e.g., the Dutch court in the TorRAT case [348].

Deviant security controls with cyber criminals as exclusive addressees are very much specialized *services*, instead of tailor-made or mass-made products. These practices may deviate from their law-abiding counterparts that offer an identical product. BPHs use the same kind of dual-use hardware and software as legitimate hosters for their dedicated and virtual private servers, but make these IT objects bulletproof against responses from the cyber security community with their administrative security services such as handling incoming abuse notifications. Likewise, bulletproof connectivity providers use regular servers and network technologies, but do not register their company, log traffic or comply to information requests of LEA. The services of crypters - also called packers - consist of using widely available obfuscation software, implementing it on malware to conceal its purpose and subsequently testing the obfuscated malware on counter-AV services. These CAVs, in turn, offer a specialized service to the underground economy, namely using bonafide antivirus products in offline sandboxes, and sending the results of their test back to their criminal clients. A last observation about tangible and intangible valuables - whether serving commission or protection, as a duals-use security product or a specialized DevSec service - is that they may lead to *tangible* and *intangible costs* which is further explained in Table 5.7.

A situation in which...	...an intangible asset leads to...	...a tangible asset leads to...
...an intangible cost:	Malware source code is leaked on the open Internet.	Talented malware developer of an organized cyber criminal group is arrested.
...a tangible cost:	Fierce competition in the underground economy leads to lower prices for e.g., ransomware-as-a-service.	Money mule group does not hand over withdrawn money to malware developers.

Table 5.7: Situations may occur in which intangible and tangible assets lead to intangible and tangible costs. For example, malware source code is an intangible asset of an organized cyber criminal group. When the source code is leaked, the group will likely lose revenues as either the cyber security community can study the malware and find solutions against it, and/or other cyber criminal groups will use the leaked malware to target potential victims first. In short, an event related to an intangible asset led to intangible costs.

5.6 Interim Conclusion and Discussion

The purpose of this chapter was to describe and explain the basic normative and empirical qualities (*what*), more specifically the definition, meaning, provision, function and form of deviant security. The findings of this chapter suggest that cyber criminals have to be able to protect *anything* which is an impossible task as perfect deviant security does not exist. This insight holds significant implications for understanding how law-enforcement agencies can deal with DevSec practices which are discussed in more detail in Chapter 8.

On the definition for DevSec This study argues that the *definition* for DevSec is solely a legal issue. Referent objects of deviant security are those natural and legal persons who are criminally liable for the commission of crime. Their countermeasures to protect the criminal and his/her crimes are what we call in this study deviant security practices. These persons knowingly violate substantive law without justification, and are therefore a legitimate target of procedural law and investigations of law-enforcement agencies. Subsequent legal analysis of national and international substantive and procedural law from respectively the Netherlands and the Council of Europe reveal that most forms of deviant security practices are criminalized with the exception of technical countermeasures of a defensive nature, while most DevSec practices are mentioned in explanatory reports of procedural law except technical countermeasures of an offensive nature. To develop a full picture of the legal aspects of DevSec, not only more legal sources should be analyzed such as case law, customs, and comments of legal scholars. There is also a need for comparative legal studies on protection of cyber crime, just as there are similar studies comparing substantive laws of different countries related to the commission of cyber crime [393][394]. In other words, comparative legal research may shed light on the differences and similarities between national legal frameworks - e.g., common and continental law systems - related to the security practices of cyber criminals. In which jurisdictions and under what circumstances is, for instance, the usage of encryption for deviant security purposes criminalized? Have national legislators ever mentioned offensive technical controls to justify the introduction of new investigative powers?

On meaning and provision of DevSec This study further provided evidence that the normative definition for DevSec is empirically observable. Not only may the security practices of cyber criminals truly deviate from good guy security, the findings of this study also prove that DevSec is empirically measurable in a qualitative manner while arguments are given why DevSec is further measurable in a quantitative fashion. So besides more legal scholarship, there is abundant room for progress in a number of other disciplines, using a variety of data sources, methods and techniques. One of such new areas is the psychology of deviant security, using - amongst others - interviews to learn what (convicted) cyber criminals think about their own and others' deviant security. This approach is based on the *meaning* of DevSec as a state of being, more specifically a subjective condition that refers to the feelings of cyber criminals about their own security. The questions for this new field of study are numerous. In which mental state do cyber criminals make more failures and mistakes? What effect do advertisement banners of DevSec providers have on forum members? What do cyber criminals consider to be their most important (protective) asset, and why? Because security practices of cyber criminals are empirically observable and deviant from practices of law-abiding citizens, more research will also help attribution as e.g., stealth can also be revealing [19, p.20]. Research is further needed on the relation between intent of suspects and their level of deviant security. The current study also described the *provision* of DevSec, either as a common, club, private and public good. Related to the latter two goods is the misusage of cyber criminals of commercial and free legitimate services like social media [395]. Yet it remains unclear how cyber criminal misusage exactly deviates from the legitimate usage by law-abiding referent objects as a limitation of this study is the fact that it had no access to customer databases of legitimate companies. Lastly, more research is needed on how multilateral security is achieved within cyber criminal communities. Which individuals or what events brings conflicting security interests to light, and what strategies do forum admins and significant others deploy to, for instance, negotiate compromises?

On function and form of DevSec Before describing the *function* of DevSec, namely an asset to protect other assets, this chapter provides an extensive taxonomy for assets. This taxonomy is not only applicable to assets related to the commission of cyber crime, but also to assets related to the protection of cyber crime and the cyber criminal. This means that its *form* is tangible and intangible as well, and comes as a duals-use security product or a specialized DevSec service. Further socio-technical studies may focus on the proportion of human, organization and information capital on CaaS markets. Which topics are most discussed, which products/services are most offered, and what is the equilibrium of admins/moderators to members/postings? More work is further required to determine the financial value of tangible and intangible assets of profit-driven cyber criminals, and costs and profit margins of DevSec products and services on the CaaS market. Qualitative research may explore how pricing works in the cyber criminal underground economy. Hopefully, mixed method approaches may answer if cyber criminals hold security budgets and an upper cost ceiling that they will not break. Ultimately, based on seized data sets of markets like Alphabay, Hansa or Darkode, future studies might measure the financial value of secure platforms, and understand which intangible assets of the platform represent the most value to the community such as a well-functioning reputation or dispute resolution system, or a seller with a unique product or service that attracts new members to the market place.

Chapter 6

Who? - Interactive Qualities of Deviant Security

We now move on to the interactive qualities of DevSec. As depicted in Figure 6.1, the following narrative of key players, their inter-relationship and the interplay between associated vulnerabilities and countermeasures is generated from the ground truth data. Firstly, three groups of key players of deviant security are categorized and described without discussing their interdependence, more specifically the i) referent objects of deviant security, ii) providers of DevSec and iii) threat agents to the protection of cyber criminals. The chapter then explains their inter-relationship, i.e., the nature of the intertwined networks in which these key players operate, and the related vulnerability of information asymmetries between key players. The latter weakness is fueled by the countermeasure of deception which creates new vulnerabilities that in turn have to be patched by trust and distrust mechanisms. In other words, vulnerabilities can cause *snowball effects* that lead to a *vicious circle* - i.e., downward spiral - in which one weakness and related countermeasure generate multiple new, and sometimes even graver, vulnerabilities.

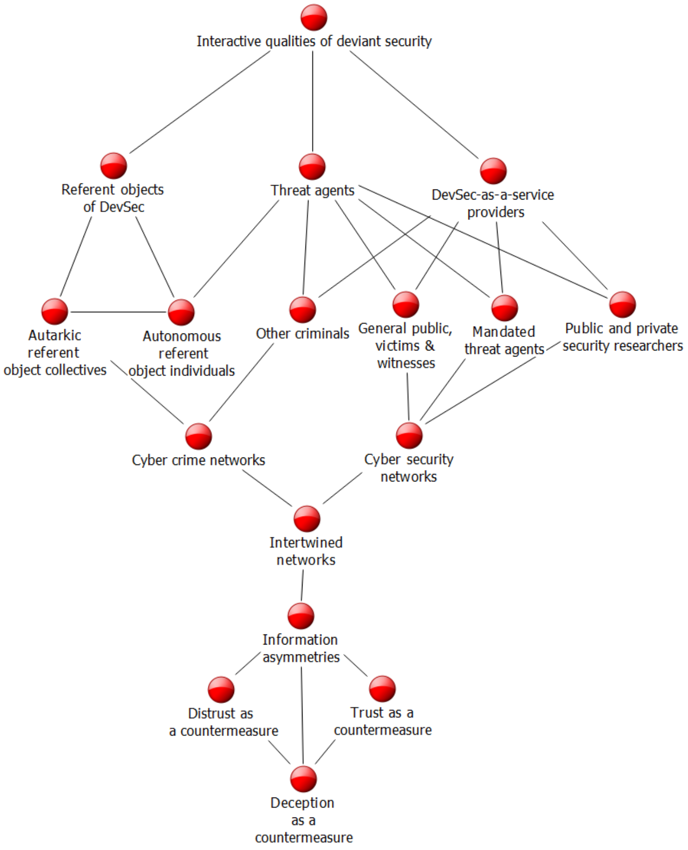

Interactive qualities of deviant security
Referent objects of DevSec
Threat agents
DevSec-as-a-service providers
Autarkic referent object collectives
Autonomous referent object individuals
Other criminals
General public, victims & witnesses
Mandated threat agents
Public and private security researchers
Cyber crime networks
Cyber security networks
Intertwined networks
Information asymmetries
Distrust as a countermeasure
Trust as a countermeasure
Deception as a countermeasure

Figure 6.1: This visualization shows the structure of Chapter 6 via a selection of key concepts about the interactive qualities of deviant security. For a full oversight of descriptive and explanatory key concepts of Part III and their inter-relation, see Figure 9.4.

6.1 Autarkic & Autonomous Referent Objects

The first category of key players are the referent objects of deviant security. Cyber criminal collectives on a meso level - whether the larger cyber criminal community or a specific cyber criminal organization - are to a certain degree autarkic when it comes to their protection. On a lower, micro level of aggregation, individual cyber criminals have to be autonomous in their security as they cannot rely on others for their security.

Autarkic cyber criminal collectives All criminal communities are to some extent *autarkic* in their security, yet some communities are more independent and self-sufficient than others. For example, sexually-driven CSAM platforms, as compared to financially-driven CaaS fora and cryptomarkets, do not have vendors that offer commercial deviant security services [385]. Review of relevant investigations and conversations with investigators paint a picture about the members of CSAM communities who solely rely on themselves and their co-conspirers for coming up with security policies and implementing them correctly. Hence, security threads and postings are constantly updated as CSAM offenders need to be up-to-date about the latest threats and vulnerabilities, underlining the idea of deviant security as a continuous activity (i.e., pursuit) and club good. While commercial online CSAM shops, file-sharing services and fora might make use of protective services such as rogue financial handlers and bulletproof hosters, LEA encountered several non-profit CSAM fora that were hosted on home servers (nota bene, no data is found of CaaS fora and/or cryptomarkets that were hosted on home servers). The explanation for the latter might be that many BPHs explicitly forbid CSAM on their servers, and/or that CSAM users tend to keep their collection - an asset which has emotional and sexual value to them - physically close to them [194, pp.148-170]. A degree of autarky is not an exception for smaller units, like cyber criminal organized groups. While some organizations try to keep the group as closed as possible, and develop and execute as many parts as possible of their MO themselves (one of the key differences between the Carbanak and Buhtrap group: the latter outsourced more of their work as compared to the former), even the most advanced Russian-language groups cannot avoid contracting out some of the security they need [396]. Similarly, the Dutch TorRAT group had started largely autarkic, but increasingly bought services and products from the underground economy, like bulletproof hosting, CAV and malware obfuscation [397]. Thus, there is a tradeoff between *autarky* of the collective versus *outsourcing* of deviant security to outsiders of the collective. Notably, some vendors on the CaaS market jumped in on this tradeoff, and offer a balance by providing do-it-yourself DevSec services. Some fake document providers, for example, may have their own websites on which customers can create their own fake passport, driver license or other identity document [398].

Autonomous cyber criminal individuals All cyber criminals are to some extent *autonomous* in, and thus responsible for, arranging and executing their own security. As described, each individual has his/her own specific deviant security interests. Therefore, an individual cannot rely on the larger community or the group for his/her deviant security, and need some self-governance of their protection without outside control as their security is seen by others as a *negative externality*. A developer that sells his/her malicious software on the underground economy might not care if there are any vulnerabilities in his/her malware that are exploitable by threat agents. His/her clients will probably take the true punch as their botnets install the malware on victims' systems and as such take the biggest risk of getting detected. Botherders, in turn, rather attack the networks and machines of third parties with their botnet, and not the owners of the infected machines, to avoid detection and thus loss of the asset of a bot [357][162, p.17]. Similarly, several breaches of client databases of vendors in the underground economy were observed during this study. However, the owners of the databases did not inform their customers. They have no incentive to do so: complying to any informal underground data breach notification law would harm their credibility and result in a *competitive disadvantage*. Therefore, individuals have to strike a balance in their security between *cooperation* with others versus *autonomy* of the individual. Security interests as *confidentiality, unobservability* and *anonymity* (read: protection of identity) express a preference for autonomy. Even for security interests that are needed for cooperation like *availability, accountability* or *authenticity*, individuals need a degree of autonomy to check any related security violations [64, pp.47-49]. Thus, a referent object has to undertake at least some of his/her deviant security without outside control, and will always bear some *implementation costs*.

6.2 DevSec Providers & Services

The second group of key players are suppliers of deviant security. Providers of DevSec can be divided in those who intentionally deliver deviant security and those who unintentionally provide it, and are found across both cyber criminal and cyber security communities. That the division between intentional and unintentional providers is not black and white, but rather forms a continuum, is shown by one of the most important aspects of cyber crime: the (mis)usage of Internet hosting services. As compared to other legitimate and illegitimate services, servers are absolutely vital for the commission of cyber crime. In other words, while sexually-driven computer-assisted CSAM users can go without money laundering and financially-driven computer-enabled drugs vendors without fake documents, *all* computer-enabled crimes and most other cyber crimes are depending on domains, IPs and servers. Yet the behavior of hosting providers may widely differ in the level of technical computer security towards cyber criminals and be classified in legal terms such as culpability and liability as shown in Figure 6.5.

Intentional providers Deviant security may be complex, labour-intensive and time-consuming for referent objects. Malafide individuals and organizations might decide, for example, that they cannot or do not want to bear any *development costs* of deviant security controls. As a result, DevSec has become a sellable asset. So, not only the commission of crime consists of specialized and deskilled divisions of labour [34], but also the protection of the criminal and his/her crimes to the extent that there is a *DevSec-as-a-service economy* in the cyber criminal underground as shown by Figure 6.2. Service providers, who operate on this market and *knowingly* provide DevSec, include hosting and connectivity providers, counter AV vendors, crypters, escrow service providers, malware developers that do security-by-design, and deviant security consultants (see Table 6.2 for a full list).

Deviant security practice	**Section**	**DevSec-as-a-service providers**	**Description and/or service examples**
Trust and distrust countermeasures	6.6	Escrow	Provide trust between vendors (read: supply) and clients (read: demand).
		Counter antivirus	Test malware to prevent detection by legitimate AV software, as a separate service or integrated in e.g., exploit kits.
		Credit card checking	Test if stolen credit cards are blocked by financial institutions.
Countermeasures against data volatility & retention	7.1	Crypting	Obfuscate and/or resize code to prevent detection & add functionalities to detect debuggers and virtual machines (VMs) of security researchers (see e.g., [399, p.3]).
		Preloaded/configured VMs	Deliver virtual machines that are purposely build to securely commit crime by avoiding data leakage about the criminal and his/her crimes. Frequently combined with other countermeasures such as deception tactics, e.g., leaking disinformation, and integrated connectivity services like VPNs (see e.g., [400][401]).
		Telecommunications	Deliver phone (prepaid or subscription) with business enterprise server, encrypted communications and/or anti IMSI catching.
Distribution as a countermeasure	7.3	Hosting and connectivity	Obscure the location of servers, handles abuse notification, and provide secure sockets layer (SSL) deployment and IP spoofing. Provide SOCKS, Layer 2 Tunneling Protocol (L2TP) and (other) VPN protocols without revealing customer details to LEA and/or logging traffic.
		Online money laundering, like cryptocurrency tumbling & obnal	Conceal the origins of illegally obtained money, typically by means of transfers involving foreign banks, legitimate businesses [402], or accepting criminals' cryptocurrencies and randomly exchanging cryptocoins for other users' coins to obfuscate their ownership (see e.g., [403, p.486-487]).

		Reshipping-as-a-service and other offline money laundering	Serve as ‘relaying intermediaries who cloak the criminals’ true identities. [...] These schemes act as an additional level of indirection and obfuscate traces that the criminals might have left behind otherwise’ [212, p.1082].
Deception as a countermeasure	6.5	Domain name registration	Provide domain name protection: domain generation algorithm, (double) fast flux and false WHOIS credentials.
		Fake documents	Produce false documents such as passports, IDs, drivers licenses and official legal documents (see e.g., [197, pp.158,167-168][404]).
		Account verification	Provides verification via e.g., phone/short message system (SMS) to register email, chat and other accounts on platforms of legitimate services.
Physical countermeasures	7.4	Hardware modification	Spoof unique IDs of hardware, like international mobile subscriber identity (IMSI) and international mobile equipment identity (IMEI) numbers and media access control (MAC) addresses.
		Prevention-of-prosecution	Prevent prosecution after arrest by means of bribery.
		Physical security controls	Detect, deter and disrupt intruders with physical security controls such as CCTV, jammers and scanners. These controls are mostly sold via spy shops that may also connect clients to providers of technical offensive countermeasures, like hackers.
Technical offensive countermeasures	5.1	Denial-of-service	Execute a range of attacks such as telephony denial-of-service, distributed denial-of-service, email flooding, IMSI flooding, and buffer overflow.
Human capital	5.5	Deviant security consultancy	Formulate and/or implement DevSec policies and mechanisms to clients.

Table 6.2: An oversight and description of the various DevSec vendors and their products and services in the CaaS underground economy, including the DevSec category in which these products and services fall. Be aware that some services and products are also offered by bonafide vendors on the regular IT market, yet in another, i.e., legitimate capacity.

As said, states can be intentional providers of DevSec as well, and turn security for criminals into a public good. Besides (geo)political reasons that are explained in detail in Section 7.3, states may also have other incentives to tolerate DevSec practices in general and more specifically the DevSec-as-a-service economy. This happens, for instance, with secure communication platforms. These may not be taken down when LEA and intelligence services have acquired a valuable information position after considerable efforts. Criminals may also openly show their activities in states without the rule of law, using extreme violence and the installment of a security apparatus [283]. Such an apparatus consists of a network of bribed police officers, judges and politicians that provide a 'roof' to suspects (крыша - 'krysha' in Russian) [320, p.10][364], to the extent that обнал ('obnal' - i.e., money laundering for bribery purposes [376][405]) and prevention-of-prosecution are offered as a service on cyber criminal fora [343]. Police officials in the Silk Road investigation obstructed justice by offering counter-intelligence on law-enforcement to the administrator of the forum [406]. Individuals misusing their diplomatic status to commit cyber crime have also been observed during this study, as well as cyber criminals that commissioned legal attacks by corrupt law-enforcement officers on malafide competitors and legitimate private security vendors to protect their illegal activities. In all of these examples, state protection as a private good is delivered by government officials to cyber criminals. The private security industry may also willingly provide DevSec. During a joint public-private investigation of the police and a private security company into online bank fraud, a competing security vendor knowingly published a report about the same malware. Immediately after the launch of the report, the criminals altered the configuration of the malware and avoided the usage of ISPs in certain jurisdictions which negatively affected the investigation. Lastly, other stakeholders in the cyber security community - most notably witnesses and victims - may provide security to criminals by, for example, altering statements, or not filing a complaint [80, pp.85-86]. The latter is apparent in cyber crime cases, like ransomware, in which victims have few incentives to file a complaint although the victim and his/her computer might hold investigative leads for the police [407].

Unintentional providers Actors within the cyber security community - notably, states, the private security industry and other stakeholders - can also be *unintentional* providers of deviant security. Legislators and policymakers may write laws or policies that not only protect the rights of the individual, such as the attorney-client privilege, but might also hold unexpected consequences that protect malicious activities. Traditional criminals added attorneys in email discussions by default, sent legal interns to criminal meetings [408], and shipped narcotics in letters with logos of law firms. Accidents, mistakes and failures might help criminals as well. A uniformed police man asked a suspect of an investigation during a routine check if he was related to cyber crime 'because the police system says so'. Police and CERTs that unknowingly sent information and/or notice-and-takedown requests to bulletproof hosters that

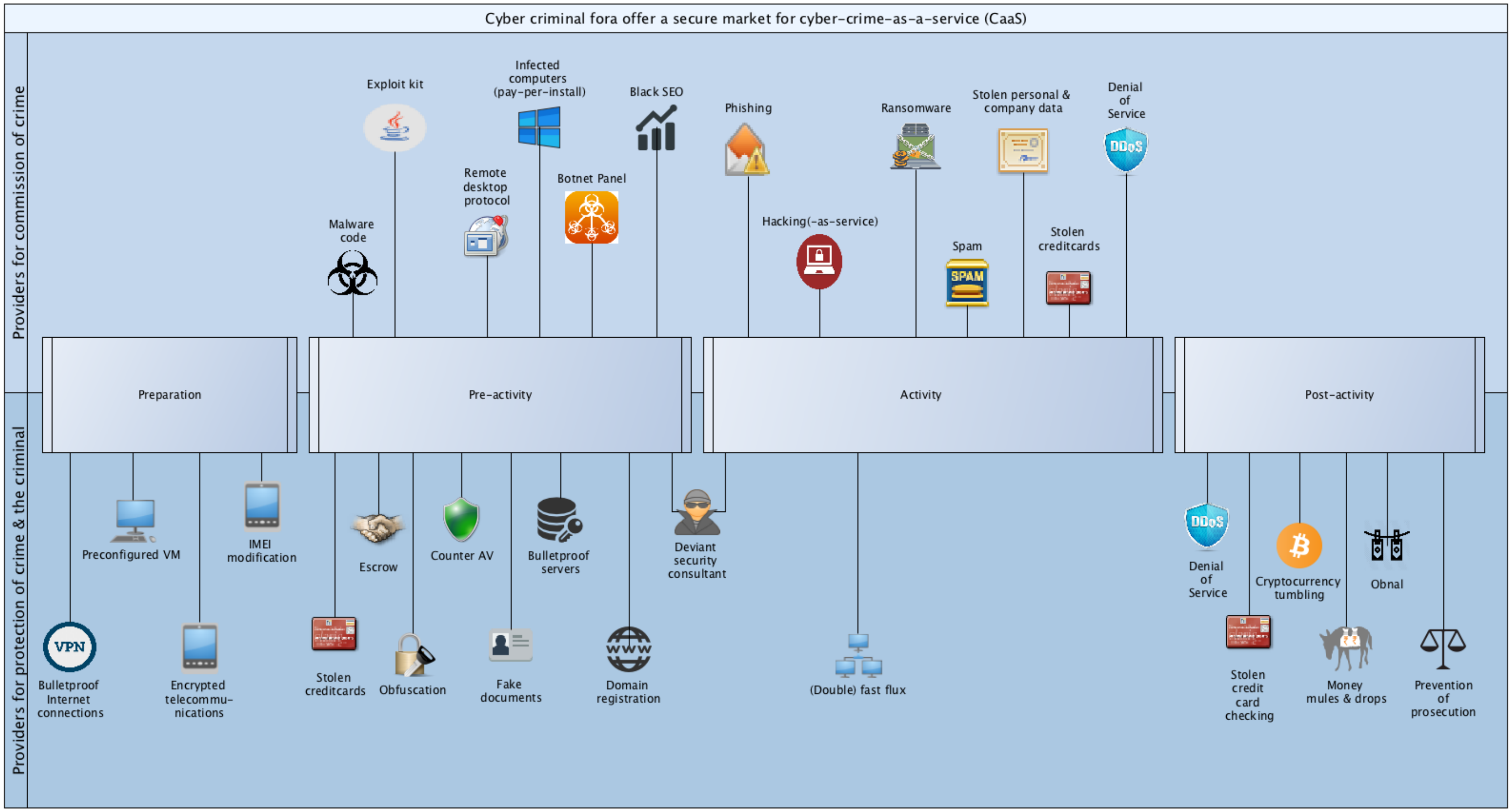


Figure 6.2: This simplified crime script analysis displays the services offered on Russian-language cyber criminal fora that predominantly facilitate financially-driven computer-focused crimes. Each service serves a specific purpose in the preparation, pre-activity, activity and post-activity of the commission of crime, and the protection of crime and the criminal. Some of these services - denial of service (like DDoS and email flooding) and stolen credit cards - serve both commission and protection. Compared to products/services that only serve the commission of crime, DevSec services/products are especially apparent in the preparation and pre- and post-activity phases. Notably, many commission and protection providers advertise services that are closely related to their core business. For instance, some bulletproof hosters not only sell servers, but also offer VPN connections, domain registration, DDoS protection and (double) fast flux. In other words, these suppliers increasingly provide integrated, full-service packages.

in turn told their criminal clients that they were a target of law-enforcement agencies. A DevSec-as-a-service provider has been observed that sold a service in which governmental institutions unintentionally helped out. A cyber criminal claimed that he had hacked multiple police systems, subsequently provided evidence of his access, and offered information from these systems for sale. Security researchers accidentally sent false positive indicators of compromise (IoCs) to banks, turning the banks' focus away from the attackers. Technologies of bonafide technology and security vendors are misused by criminals for protective purposes - such as Brazilian cyber criminals who use legitimate social media to communicate [409, p.2], cloud services to host C&C servers [410], or cyber criminal fora using DDoS protection of a legitimate service provider. Victims might contribute by not being forensic ready, like having installed IDS and audit systems, which seriously hampers private and public investigations after a successful attack. Lastly, a fire in a datacenter destroyed hardware for lawful interception and historical subscriber information [411]. How should those who are confronted by deviant countermeasures regard these challenges? All the examples point to a twofold setback for the cyber security community, i.e., the *double whammy effect of deviant security*. The cyber security key players not only have to overcome the security practices applied by the criminal, but also their own, self created barriers and those of significant others, that help criminals in commission and protection. Many of the underlying causes of the current effectiveness crisis in traditional investigations are also present in public and private cyber crime investigations. These challenges are mainly of a political/legal and organizational nature [412], such as too many unnecessary bureaucratic rules, absence of strategy and coordination, internal and external conflicts, mismanagement, loss of operational momentum, poor skill sets and professional attitudes, and fierce rivalry within the cyber security community [12][413][228, pp.64-65, 98-100][414][415].

6.3 Threat Agents & Attacks

The third group of key players of deviant security are threat agents. Each type of cyber crime - whether computer-focused, assisted or enabled; politically, profit, sexually or thrill-driven - comes with its own risks to the criminal's assets, read: threat agent and related attacks. These breachers of deviant security consist of a wide variety of actors within and outside the cyber security community, more specifically mandated threat agents, (victim) witnesses, public and private security researchers, other criminals and referent objects themselves. Some threat agents and attacks will have a significantly lesser impact on the referent object than others. Fraud by a ripper only leads to an unfortunate but single monetary loss. Public leakage of the malware source code by a disgruntled insider (e.g., developer) or thrill-seeking outsider (hacker) results in continuous loss of revenues, while doxing by vigilantes or competitors causes permanent damage to the criminal's true identity. While most examples in this section are about threat agents who intentionally breach the security of cyber criminals, there is also evidence of unintentional breaches. An ISP, for example, accidentally run an autoscript that deleted all data on an important server of a cyber criminal group.

'Please do not touch my CSAM server'
An investigator and prosecutor told the following story about a system administrator of a company who had stored his CSAM collection on a server at work. Presumably, he did not want his colleagues to physically touch his server. He therefore attached a plastic name label on the server so others would leave the server alone. However, when LEA investigated him, officers could easily find his server in the company's rack frame. The label also provided evidence that the server was truly his. The CSAM user in this example faced a zero-sum security tradeoff. The name label did not create a situation in which he would discourage both types of threat agents. On the contrary, his gain of scaring off colleagues with a name label meant a certain loss when law-enforcement officers would need to locate the server and subsequently attribute the server to him. Similarly, a BPH labelled his servers that were blacklisted by the private industry to protect these IT focused assets, but simultaneously provided evidence for LEA that he had knowledge about the malicious activities of his clients on these servers. Lastly, many suspects during this study were encountered that saved all their writings with other cyber criminals as proof about e.g., the negotiated terms and conditions of (potential) business transactions. When alleged violations of agreements occur, transaction partners can demand arbitrage of forum admins and present the writings as 'evidence'. The same writings that can also be used as evidence by legal practitioners against them in court.

Mandated threat agents Some key players - predominantly state agencies - have a public legal mandate to launch offensive attacks against suspects of crime. These public agencies wait for, and exploit, any failures and mistakes of cyber criminals, and breach DevSec. Police investigations primarily focus on tracing back the true identity of their suspect, and will subsequently streamline their strictly regulated interception, interruption and fabrication attacks as such. Some regulators, like the United States' Federal Trade Commission and the Netherlands Authority for Consumers and Markets (ACM), have legal powers to investigate a limited number of specific cyber crimes like the act of sending spam messages. Likewise, the US Federal Communications Commission and the Radiocommunications Agency Netherlands have the legal authority to investigate distributors and users of GPS and cell phone jammers - a physical deviant security control. Financially-driven individuals who also conduct state-sponsored espionage - as well-known suspect with monikers Slavik and lucky12345 allegedly did [416] - or cause large damage to national critical infrastructures - like the WannaCry ransomware did [417] - might become targets of intelligence services that have far reaching surveillance powers. Hence, a review of advertisements and terms and conditions of bullet proof hosters show that most of these DevSec providers try to avoid becoming a threat agent to state security, thus a target of intelligence services, by explicitly forbidding terrorism and/or anti-government related activities on their servers. Still, this prohibition may be ignored by clients. BPHs have been (mis)used as criminal proxies in a number of state-sponsored attacks to create *political plausible deniability*, namely: the use of deception tactics - маскировка ('maskirovka') in Russian, false flag attacks in English - to disguise intelligence, military or state-sponsored attacks (see also [418], and the BlackEnergy crimeware used in politically-driven espionage against Ukrainian government institutions [419]).

(Victim) witnesses Witnesses of cyber crime, including victims, are individuals within public and private organizations and the general public (child victims, coincidental bystanders, concerned citizens, family members, neighbors, etc) who are confronted with cyber crime. Some breach DevSec unintentionally such as girlfriends who use their boyfriend's VPN connection (which is intercepted by LEA) to login to social media revealing her true identity. Observed examples of intentional breaches of physical deviant security by the public are victims of CSAM that disclose the abuse to others, or family members and friends that discover CSAM on a home computer, revealing the activities and/or identity of the perpetrator. Similarly, evidence from reviewed investigations and media reports show that communication, financial and security products/services of legitimate companies are frequently misused for criminal purposes [395][420][421]. Several organizations did step forward and informed and/or collaborated with LEA about these activities during this study. From a legal perspective, the knowledge of (victim) witnesses about crimes can become evidence in criminal proceedings through the form of victim and witness statements. Yet they might be exempted to give evidence when they are legally allowed to do so, such as marital privilege. Moreover, victims and other plaintiffs can start civil lawsuits against cyber criminal defendants, like a software vendor did against operators of - amongst others - the Kelihos, Rustock and Zeus botnets [422][423][424]. Not only can civil lawsuits be brought against defendants to compensate for the financial losses caused by the botnets, but plaintiffs can also obtain court orders that permit to seize botnet assets like domain names and hardware without first notifying the owners of these assets [425].

Public & private security researchers A special category of witnesses are academics, abuse hotlines, attorneys, investigative journalists, NGOs, private and public CERTs, regulators, employees of the private security industry (like antivirus vendors and private investigators - called contracted security) and corporate security such as cyber threat intelligence departments of large enterprises (called in-house security). They too pose a security threat to cyber criminals, especially by pro-actively gathering information about the security of cyber criminals, and subsequently reporting about their vulnerabilities. Besides commercial aspects, there is a big difference between private and public security parties. The former is able to install intrusion detection systems on their clients' machines, while some of their public counterparts also focus on commercially less interesting targets including DevSec providers like bulletproof hosters. In other words, both groups have their own unique information position. The attacks by security researchers (also called defenders from a good guy security perspective) are mostly defensive, but sometimes also offensive: think of an incriminating news report about a malware author by an investigative journalist [426], botnet sinkholes by non-profit organizations [427], or academics who couple machine learning methodologies with information retrieval techniques to crawl carding shops, fora and chat channels on - amongst others - the Dark Net [428][429]. The threats of public and private security researchers include technical and non-technical attacks of fabrication, interception, interruption and modification. These attacks harm the availability, integrity and confidentiality of criminal assets. The former includes the removal of infected computers in a botnet and/or takedown of C&C servers [159], the middle points to DNS sinkholes to obstruct the use of C&C domain names, while the latter refers to news articles that uncover the hidden world of cyber criminals and their crimes. Public and private security researchers too might be exempted to give evidence when they are privileged to do so based on e.g., attorney-client privilege like legal practitioners, or data protection laws like journalists and scientific researchers [430].

Other criminals Other criminals can be threat agents to referent objects of deviant security as well. Breaching the security of other cyber criminals is for most criminals a low-risk activity: offenders can protect their identity, while they do not have to be physically near their 'victim', nor do they have to come forward with their deeds [17, pp.445-450][431, p.178]. Furthermore, their victims will likely not file a complaint either. For example, an organized group specifically targeted carder shops that sold stolen credit card credentials. There are various motives in play why criminals target other suspects of crime: competitors intend to harm the business of their rivals; hacktivists are motivated by ideological goals; rippers are financially driven; and vigilantes want to initiate prosecution. Throughout this study, examples are given of attacks by these threat agents against assets of other criminals, including their security. Less obvious criminal threat agents to malafide assets are pirates of 'criminal intellectual property'. Unauthorized malware is offered for sale on the underground economy like the pirated versions of the ransomware-as-a-service Philadelphia [432, pp.22-28]. The developers of both Carbon Grabber and SpyEye therefore installed protective measures, including backdoors, against those who used an unlicensed copy of their malware [433][434]. The individuals behind the Blackhole exploit kit protected their malware code with a commercial encoder for a similar reason [435]. While cyber criminals commit a range of computer-focused, computer-assisted and computer-enabled offenses against other criminals, an act with far reaching consequences is revealing identifying details of their victims (known as doxing) as this affects the confidentiality of the precious identity asset of a criminal. Indeed, cyber criminals, including hacktivists and other cyber security vigilantes [436], regularly hack their targets and leak the stolen information - sometimes complete databases - to investigative journalists, LEA or public drop boxes. This illegally obtained evidence by a third party is under certain circumstances admissible in - amongst others - Dutch criminal court proceedings [437][438].

Hacktivists against CSAM users
The fear of getting caught in combination with the need for security were exploited by hacktivist group Anonymous during a technology-based social engineering attack against CSAM users in 2011. They launched a disinformation attack on a CSAM underground forum, claiming that Tor should be updated because the privacy enhancing technology could not be trusted anymore. On the day of the legitimate Tor update, they subsequently offered a bogus software update that allowed the hackers to extract the true IP addresses of the users, and tracking their visits to underground fora. As such, the hacktivists harmed the identity assets of 190 alleged CSAM users [439].

Referent objects: breach your own security Lastly, referent objects may intentionally or unintentionally breach their own security. Because cyber criminals are always to some extent autonomous in their own security, many breaches occur because of their own self-inflicted accidents, failures and mistakes such as bad implementation of administrative security policies or malfunctioning technical security mechanisms. VPN connections frequently fail and/or are not consistently used which reveal the criminal's home IP address in netflow data [112]. Similar to the error made by the MoneyTaker group where a program developed to erase all malware traces on a victim machines failed [440, p.4], a suspect under investigation wrongly configured a server. Instead of automatically deleting the access logs of the server, all traffic was still recorded and stored. A suspect refused to hand over the password of his laptop to the police. He had, however, installed a remote access tool on the machine for testing purposes. The investigators, in turn, exploited this backdoor and gained access to the machine. Security may also be intentionally lowered to optimize malicious business proceedings. Although highly secure, Tor over a triple or even quadruple VPN connection may seriously slow down Internet access, and is therefore probably one of the reasons that this practice has not been observed during this study. Moreover, suspects have the legal privilege against compelled self-incrimination. Yet they may be inclined to intentionally give up (some of their) security after arrest by handing over incriminating evidence and/or financial assets to the police in the hope that cooperation will lower their sentence (see, for example Dutch court case [441]), to the extent that some will turn into (criminal) informants. Lastly, novices - also known as newbies or noobs - are major threat agents for cyber criminal organizations, as their failures and mistakes may have a negative impact on co-conspirers.

6.4 Information Asymmetries in Intertwined Networks

After describing referent objects, DevSec providers and threat agents, the question of this section is: what is the inter-relationship of these key players? Key players and their assets - whether human or non-human, tangible or intangible, for commission or protection, related to the criminal or his/her crimes - do not stand on their own: they interact in networks [293]. Generally, academic studies distinguish between cyber criminal networks and cyber security networks. This dichotomy between the criminal phenomenon and reaction to that phenomenon is a simplification of reality. Because applying and breaching DevSec is a socio-technical practice, the key player networks in which self-suppliers, providers, purchasers and breachers of DevSec operate, are all intertwined. These intertwined networks hold various vulnerabilities related to the identity and business operations of cyber criminals. An important vulnerability that affects the security of cyber criminals are information asymmetries between the key players of the intertwined networks. As a result, cyber criminals operate on a lemon market - a form of *market failure* - for their deviant security: they have little accurate information about the quality of their purchased security product and/or service.

Intertwined networks of key players In practice, key players have multiple identities as they are part of various groups and networks: criminal and legitimate, private and professional, social and technological. The groups and networks in which these entities operate are indeed *interconnected*, i.e., networks of networks. Cyber criminal networks react to interventions of the cyber security community after events like the arrest of a co-conspirer, the takedown of their Internet infrastructure, or the publication of a threat analysis with IoCs of their attack. The group behind the mobile banking trojan Cron, for instance, modified their malware to attack other countries than Russia after the arrest of a member in the Russian Federation [442]. In other words, networks are constantly surrounded and shaped by key players that either support or fight them [293, pp.592-593].

Because cyber criminals belong to various groups and networks, the multiple identities that they develop come into play at different times, depending on context [363, p.96]. However, managing multiple identities is extremely hard for cyber criminals. As depicted in Figure 6.3, the groups and networks of referent objects and threat agents are not only linked, but also very much *intertwined* as entities potentially hold several roles over time. Most key players can simultaneously be on the providing and receiving end of DevSec, as well as breaching it. As a result, cyber criminals are always connected to potential breachers, even in their most trusted social surroundings. For instance, DDoS attackers were identified after they bragged about their crimes to relatives of law-enforcement officers. Many law-enforcement agencies have information positions within cyber criminal networks through (criminal) informants and undercover operatives. Likewise, there are allegations of Russian law-enforcement agencies actively recruiting cyber criminals to work for them [443][252]. Cyber threat intelligence reports of other nodes within security networks - especially private security companies - may lead to the believe that they have a well-established information position on criminal networks as well. For instance, a private security company - prior to the official police investigation - publicly named several nicknames who were allegedly related to a botnet, but a cyber crime unit of the police could not identify any monikers, even after using evasive investigative powers.

Did the private security company do a very good job in open source intelligence, or did they go a step further, such as starting conversations with other cyber criminals or even went so far that they hacked the suspects' systems?

Citizen participation in police investigations further intertwines the network. For example, the general public was asked on Dutch television if they recognized the voice of a ransomware offender, and on another occasion, the face of a victim depicted on an image. Furthermore, multiple law-enforcement agencies have launched the idea of more active crowd policing projects in which citizens are stimulated to detect and report cyber crime [444]. Such ideas and initiatives add to an environment of emerging cooperative criminal justice system in which cyber security vigilantes also play a significant role [436], such as an individual that took down the Wannacry botnet who turned out to be the alleged developer of the Kronos botnet [445]. Criminals therefore need to apply security in all of their networks, as informational capital in, for example, a legitimate network might reveal the identity and criminal activities within another network. Such *contamination* of identities and activities are often breakthroughs in investigations (see e.g., [446, p.2]). Think of entities of cyber criminals - like bank accounts, chat and email addresses and/or phone numbers - that are used for both illegitimate and legitimate business/private purposes. Similarly, the arrests of two wanted Russian suspects of carding in the Netherlands were possible because one of them posted his whereabouts on his social media profile [447]. Another individual not only used an unusual greeting ('hiyas') on an access controlled CSAM forum to say hello to befriended members, but also used the word on one of his legitimate social media accounts [448]. A last argument for the intertwinedness of cyber criminal and cyber security networks is the entanglement of the underground economy with the legitimate economy. Besides obvious examples as misusing financial services to launder money, several cases have been observed in which legal entities were financially depending on cyber criminals. A law-enforcement agency had to preserve a server which was rented to a reseller of an ISP. In reply to a question of the agency, the ISP stated that they had no idea if the reseller would, in turn, inform his criminal client about the preservation. The question of the police was, however, rhetorical. The reseller - a long standing client of the ISP - was a well-known bulletproof hoster with many public reports providing evidence about this accusation. An investigator told about another case in which a postal service earned over a million euro a year from a reshipping scheme and gave its malafide customer discounts. In such situations, legitimate entities might have a hard time to say farewell to their illegitimate clients and turn a blind eye on malafide activities.

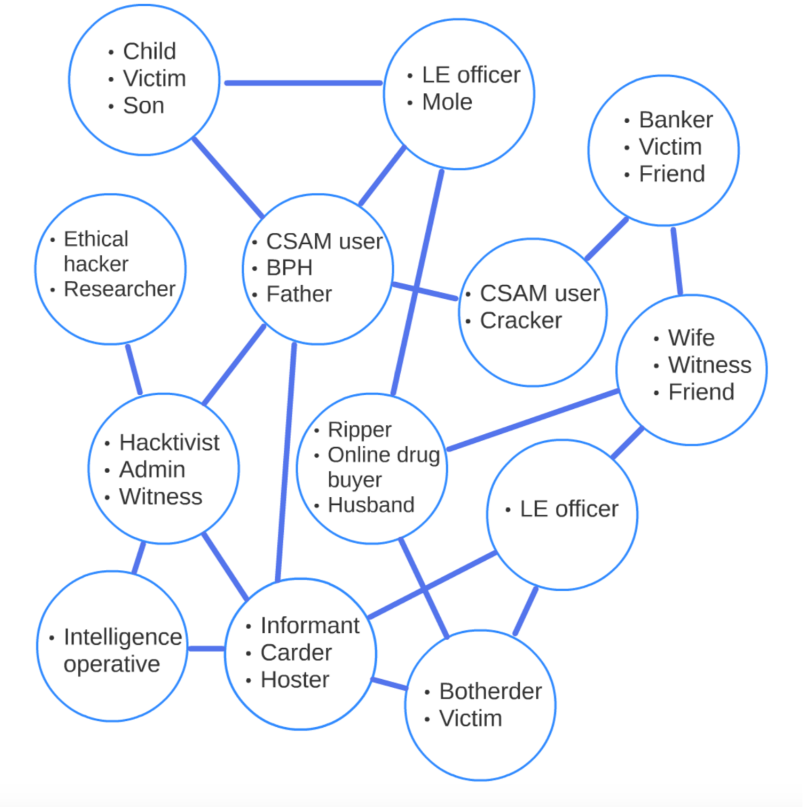


Figure 6.3: Key players - who may hold various roles - operate in an intertwined network which, in turn, creates vulnerabilities for the cyber criminal's identity and his/her malicious business proceedings. A ripper on a carder forum might reveal his own physical location when buying drugs on a cryptomarket, while his wife - i.e., a witness of crime - might accidentally reveal her husband's identity, activities or location to others in the network.

Information asymmetries between transaction partners Because cyber criminals can easily cause many small-impact victimizations distributed across multiple jurisdictions, the relationship between offenders, victims and the criminal justice system has become asymmetric [80, p.80]. But asymmetric relationships also occur in ways that do not benefit the commission of crime. Due to disinformation, misinformation and too little information about actors and their businesses [449][450], classical *information asymmetries* occur: one party has less (accurate) information about a transaction than other involved parties [451]. These information asymmetries relate to transactions of legitimate and illegitimate actors and systems with whom the criminals interact. Key players can have different roles of which the cyber criminal is not aware. Carders, for example, face uncertainties about the nature of the seller's identity, and the quality of the compromised credit cards [452, pp.522-527][453][454]. Too little information about the vendor and his/her products may harm the buyer's identity and/or business proceedings, something rippers take advantage of when cheating on buyers [186]. This does not only occur in transactions between cyber criminals, but also between cyber criminals and legitimate parties. Let us take take legitimate services that are misused for the distribution and download of CSAM to illustrate this point. Peer-to-peer (p2p) file sharing services and video media players are provided to the CSAM user by legitimate software vendors. The client, however, does not know if the company collaborates with the police or if the software leaks personal information (see [455] for victims that could read client data of a DDoS booter because that information was sent with the attack traffic. Similarly, a legitimate telecommunications application software product leaked the IP addresses of (criminal) users, see [356, pp.15-16] and [112]). The main question for a cyber criminal is in all of these transactions: is the other party friend or foe; a potential business partner or a threat agent? Because of the absence of laws that protect financial transactions of cyber criminals, the problem of know-your-customer (KYC) applies to the underground economy as well. More specifically, money launderers, including transaction anonymizers like rogue Bitcoin tumblers, do not implement anti-money laundering laws (AML) which are generally based on KYC principles [456][330][457]. On the contrary, they try to provide *relationship anonymity* [329]. Not only LEA, but both transaction partners - money launderer and client - will therefore have a difficult time to establish the true identity and motives of the other party as well.

Information asymmetries about third parties These examples are, so far, all classical information asymmetries between parties involved in transactions based on reciprocity. However, *third party information asymmetries* might also occur. Intertwined networks generate information asymmetries for the cyber criminal about an important third party that is not involved in any transaction with the cyber criminal, but unilaterally interferes with the business transactions of cyber criminals, such as mandated breachers. Online money launderers will therefore try to increase the information asymmetry between them and investigative authorities, while legislators try to decrease this information asymmetry with KYC and AML controls [330][457]. There is yet another negative side of the coin for suspects. Just as the general public lacks knowledge about the surveillance and decryption capabilities of intelligence services [458], cyber criminals have a hard time to reconstruct the investigative methods deployed in past and ongoing operations of law-enforcement agencies. As depicted in Figure 6.4, cyber criminals might unknowingly be under investigation, while LEA is successfully receiving information from other nodes in the intertwined network about the criminal and/or his/her malafide activities. This is, for instance, shown by Russian cyber criminals who traveled to various holiday destinations and who were subsequently arrested by local authorities on the legal request of the Federal Bureau of Investigation (FBI) [358]. Therefore, cyber criminals go at great length to increase the amount and quality of information about the capabilities and operations of the cyber security community, and subsequently adjust their behavior to the findings. In several instances, cyber criminals discussed newspaper articles about arrested individuals and tried to determine the online identity of the suspects. When an arrested suspect was a known contact, they subsequently deleted their current online pseudonym and changed to another nickname. The reason behind this practice is that ongoing use of their old moniker may hold the vulnerability of *linkability* (see [207, pp.21-25]) to the true identity of its holder. Because an advanced group of cyber criminals changed the location of their C&C servers immediately after a report with indicators of compromise was published by a private security company, the group presumably made use of legitimate content change detection and notification services to receive automated alerts when new results appeared on the Internet about keywords related to their assets. A more offensive and proactive stance is to develop relationships within the cyber security community, in other words, gather information through corrupt legal practitioners and private researchers.

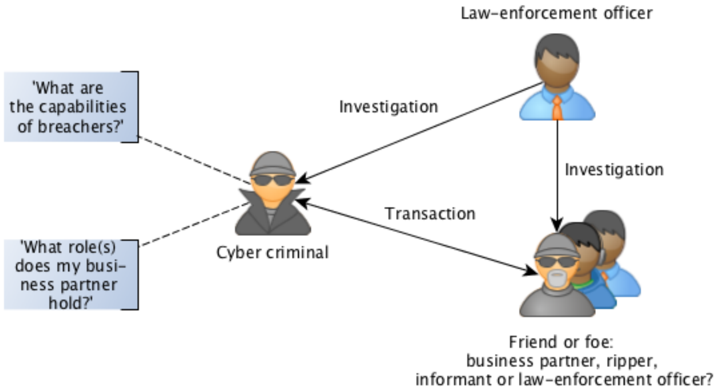
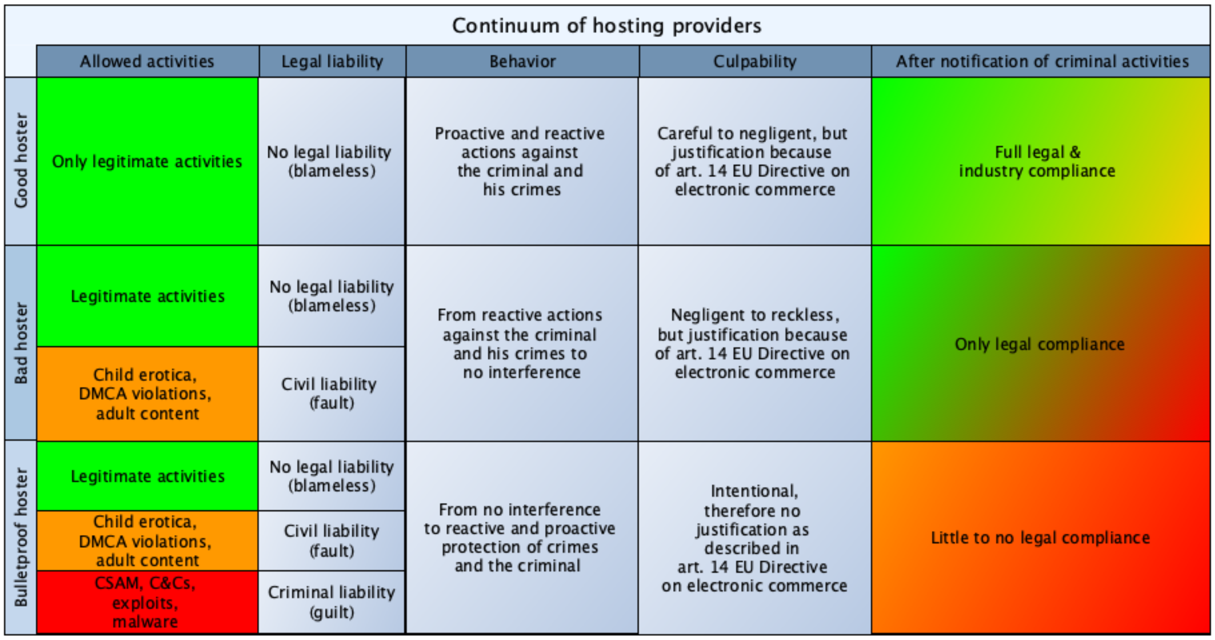

Law-enforcement officer
'What are the capabilities of breachers?'
Investigation
Investigation
Transaction
Cyber criminal
'What role(s) does my business partner hold?'
Friend or foe:
business partner, ripper,
informant or law-enforcement officer?

Figure 6.4: Two major questions for the cyber criminal about legitimate and illegitimate business partners, and breachers of his/her security: i) 'Is my (future) business partner a threat agent?' [64, p.49], and ii) 'What are the threats and attacks by known breachers, in other words, am I and/or my potential business partner being investigated by LEA?'

Vulnerabilities of information symmetries in intertwined networks
Most self-proclaimed deviant security providers - or perceived as such by their clients - apply *external secrecy*, thus confidentiality, about how they protect their customers. They provide no to little information about their business operations to their clients which, as a result, become a black box. Generally, customers seem to accept this practice as a self-evident truth. Ultimately, cyber criminals have too little information about who is bulletproof under all circumstances and who is not, and there are no effective independent quality

assurance or disclosure mechanisms. Thus, just like good guy security [182], and products and services that promote the commission of crime like compromised creditcards [186], the market for deviant security is a *lemon market*. Buyers can not distinguish between high-quality products and services (referred to as peaches) and low-quality ones (known as lemons) [451]. As such, information asymmetries add to the subjective and symbolic meaning of DevSec to cyber criminals. They might buy protective products/services that let them merely feel safe against threat agents, as compared to actual objective and material deviant security that truly protects them.

Are alleged criminal hosters truly bulletproof against threat agents?
Based on the culpability scale of [274, p.488], hosting categorization of [459, p.21] and conducting and reviewing intelligence and investigations on bulletproof hosters, this study divides Internet service providers in good hosters, bad hosters and crime hosters (read: bulletproof hosters) as depicted in Figure 6.5. Between the legitimate behavior of good hosters and illegitimate behavior of criminal hosters are the bad hosters. Bad hosters correctly reason that their system administrators cannot remove CSAM from their servers because they first have to check (and thus view) the material which is indeed *de jure* prohibited. Bad hosters further argue that they, as ISPs, are protected by laws such as article 14 of the EU E-commerce directive which prescribes that hosting providers are not legally liable for the content that they host. There are many instances in which hosting providers with a reputation in the cyber criminal underground for being bulletproof fully cooperated with LEA. These facilitators may have *economic incentives* to pass off lower quality products/services than promised to their clients. After all, availability of the complete business process is more important than the confidentiality of a single client. Other hosters accept only virtual and cryptocurrencies and evidently false subscriber details, and allow malicious content on their servers, but do not provide any further anti-LEA services to their clients. Lastly, some will also inform their customers about any abuse notifications, so the client can take necessary actions. Few will also move that content to another server. In short, there exists a continuum of seller qualities for hosting malafide activities. These examples make clear that *moral hazard* may occur in the intertwined network. Some actors, like bulletproof hosters, have an incentive to take more risks - i.e., *hidden actions* - after a deal is struck because others, i.e., their clients, will bear the (security) costs of those risks. After all, these facilitators might regard the DevSec of another referent object as a *negative externality.*



Continuum of hosting providers

	Allowed activities	Legal liability	Behavior	Culpability	After notification of criminal activities
Good hoster	Only legitimate activities	No legal liability (blameless)	Proactive and reactive actions against the criminal and his crimes	Careful to negligent, but justification because of art. 14 EU Directive on electronic commerce	Full legal & industry compliance
Bad hoster	Legitimate activities	No legal liability (blameless)	From reactive actions against the criminal and his crimes to no interference	Negligent to reckless, but justification because of art. 14 EU Directive on electronic commerce	Only legal compliance
	Child erotica, DMCA violations, adult content	Civil liability (fault)			
Bulletproof hoster	Legitimate activities	No legal liability (blameless)	From no interference to reactive and proactive protection of crimes and the criminal	Intentional, therefore no justification as described in art. 14 EU Directive on electronic commerce	Little to no legal compliance
	Child erotica, DMCA violations, adult content	Civil liability (fault)			
	CSAM, C&Cs, exploits, malware	Criminal liability (guilt)			

Figure 6.5: Be aware that especially the data centers of bad hosters may attract bulletproof resellers and other criminal customers, because of poor abuse enforcement policies and network monitoring, and non-response to industry standards such as voluntary notice-and-takedowns (NTD) of - amongst others - websites with child abuse material [460]. Another notion is that this model holds an inherently Dutch legal perspective in which intellectual property violations are not actively prosecuted, and legal child erotica (as compared to illegal child abusive material) are dealt with by voluntary industry compliance.

The market for bulletproof IP addresses, either provided by hosting and connectivity providers, is such a lemon market. Research shows that the majority of VPN services suffer from IPv6 traffic leakage [461], while reviewed investigations tell us that legitimate connectivity providers frequently log traffic and/or cooperate with LEA. Moreover, cyber criminals may get IP addresses assigned that were issued to other criminals in the past. As such, these servers are associated with illegal activities and therefore be on a blacklist of the cyber security community. To compete with these lemon providers, several bulletproof connectivity vendors with a cyber criminal forum presence offered *transparency* and set up websites that gave additional information to cyber criminals about the quality of their acquired IP addresses. Still, total honesty about deviant security practices by transaction partners is impossible as third party threat agents may benefit from transparency. Thus, DevSec-as-a-service providers have to navigate between secrecy and transparency. Moreover, good guy legal solutions to resolve information asymmetries - consumer protection regulation, external product certification, industry standards or liability laws - do not work as the cyber criminal underground is very much defined by the absence of formally enacted laws. What is left are the previously mentioned methods of increasing the amount and quality of information and installing guarantees through escrow services.

Because it is unknown what the threats are or what the quality is of DevSec products and services, it is hard for cyber criminals to determine *return on investment* for deviant security. As a result, they have a *protective asset allocation problem.* Should they opt for an approximate versus complete coverage of threats? For proactive or reactive measures on optimal configuration of their security mechanisms? For largely unaffected business processes versus an essential security overhead (see [64, p.50])? For action of developing and subsequently maintaining new deviant security controls, or inaction until current controls can no longer guarantee the expected level of protection? Given the large information asymmetries in intertwined networks, there are no metrics that provide answers to these tradeoff dilemmas. Therefore, cyber criminals easily *under protect* their assets or *over spend* on security.

6.5 Deception as Deviant Security Control

As explained in the previous section, disinformation, misinformation and too little information about key players and their acts cause information asymmetries. This section elaborates on the former cause: the distribution of false information to deliberately deceive other key players. Outright criminal or abnormal behavior, indeed even being an *outlier* for a brief moment, is a major vulnerability for cyber criminals. To protect themselves against 'standing out from the crowd', cyber criminals have to deceive other key players. As a result, cyber criminals themselves are largely to blame for inaccurate information and subsequent information asymmetries in intertwined networks. Deception is defined as the misrepresentation or restriction of information in order to influence the behaviors of others [462, p.121], more specifically, as a process through which a deceiver purposefully induces a false representation to a target [463, p.469] (see also [449][450]). In other words, deception attacks are fabrication attacks [464, p.69][54]. As a result, deception affects the *integrity* of data and related technical computer security attributes of *authenticity* and *non-repudiation* which is not only a burden to the cyber security community, but to cyber criminals as well.

Try not to stand out from the crowd An intelligence report described how a p2p botnet was monitored through a super peer that was under control of the private security industry. Among all the HTTP POST requests on the super peer, there was one GET request: the botnet herder logged on the botnet through the super peer instead of the C&C botnet panel. He further stuck out because he subsequently logged in with admin privileges which regular p2p traffic has not. Standing out from the crowd can also be understood in the literal sense of the word. When an organized group of Latvian, Moldovan, Romanian and Russian cyber criminals was busy to hack ATMs in Taiwan, Taipei citizens informed the police that individuals were acting suspiciously in front of a bank. An off-duty police officer later recognized a Latvian suspect in a nearby restaurant, and as a result, his colleagues were able to make an arrest [465].

Current scholars connect deception to the commission of cyber crime, like social engineering of victims [466][220], and to defensive responses by law-abiding entities to prevent and detect cyber criminal attacks, such as installment of honeypots [467]. So, our current understanding of deception fits very much within the dominant security course of the bad guys deceiving the good guys, and what the latter should do to prevent and detect deception attacks, by applying - in turn - security through deception [468]. The emphasis in these studies is on malicious deceptive acts that make victims, and are primarily driven by sexual, thrill-seeking or financial purposes. However, *all* malicious deception tactics hold protective qualities, and can be categorized as i) deceptive tactics to commit crime but with protective side effects, and ii) deceptive tactics solely for deviant security purposes.

Deception with protective side effects Let us first study the current academic perspective on deception attacks by cyber criminals in detail. Two observations become apparent. Most papers - with few notable exceptions like [469] - consider the target of deception attacks to be a (potential) *victim of crime* [463, p.469][470]. Secondly, most papers focus on (preventing and detecting) cyber criminal deception *attacks* on those victims, such as the use of Trojan horses, IP-spoofing, ripping, spam marketing and social engineering techniques [209, p.62][471][464][453]. In short, deception is predominantly regarded as part of the commission of crime [79, p.4], especially to increase the conversion rate of the attack against victims [150], and thus part of the good guy perspective on security. Few studies, however, consider the DevSec-related side effects of these attacks. Once the deception attack is completed and a victim is made, threat agents to the cyber criminal may respond, but are obstructed in their efforts due to the very nature of deception attacks. Deceptive crimes do not only sideline victims who have solely defensive capabilities, but mandated breachers as well, most notably law-enforcement agencies. Deception tactics further have the potential to breach the security of law-abiding victims, and without any additional efforts enhance the perpetrator's security against (potential) threat agents *after* the crime has been committed, usually private and/or public investigators. Thus, although deception attacks are solely launched to commit a crime for sexual, financial or thrill-seeking reasons, they also simultaneously have a beneficial side effect for cyber criminals as these attacks hold protective qualities as well.

Why do these commissions simultaneously have protective outcomes? Johnson and his colleagues refer to the actions of the deceiver as deception tactics. They describe these tactics by reference to a deception core, which is the item that the deceiver either intends to hide from the target, or whose fictitious properties the deceiver intends to simulate [472, p.361]. From a DevSec perspective, the terms core and item translate as all *tangible and intangible assets related to the criminal and his/her crimes* (see Table 6.3). Everything that points to the true identity of the cyber criminal and his/her financial, thrill-seeking or sexual behavior, would alarm a potential victim. To successfully commit his/her crimes, a cyber criminal must apply deception tactics to shield his/her true identity and the actions that reveal his/her true intentions. In order for an individual to groom a child, he/she might add, alter or remove certain identifiers to enhance the credibility of his/her character and achieve his/her sexual goal [473]. However, masking age, mimicking a youngster, and inventing a credible character to sexually groom a victim will simultaneously enhance his/her security against any responses from other threat agents. Similarly, job scam services request a curriculum vitae and copy of the passport of unwitting moneymules to appear as legitimate companies [212, pp.1082, 1084, 1085], and the spam emails of the Pony spear-phishing campaigns that impersonated well-known companies by using their logos and known subject lines [474]. Besides that personal data are used to commit other crimes, requesting a copy of the victim's passport works also as a countermeasure. Law-enforcement agencies will have difficulties to pose as potential employees as there are legal obstacles to create and send fake personal details like passport copies. Using hacked servers for botnet command-and-control purposes does not only benefit the commission of crime as this practice saves money, but also because all registration and payment details of the misused servers lead to an innocent party. These examples show that deception attacks with protective side effects are always of an offensive nature (hence, the use of the word attacks), and hold deterrent and preventive functionalities: they help to discourage potential threat agents, and stop successful completion of attacks on the security of the cyber criminal. Because many offensive deception attacks are illegal (e.g., phishing) but inherent to the MO of suspects, cyber criminals would hypothetically enjoy more security than their law-abiding counterparts whom cannot rely on the same deception tactics.

Deviant security through deception	**Tactic**	**Definition**
Hiding the real: Prevent an accurate understanding of the deception core, i.e., *the criminal and his/her crimes.*	Masking	Eliminating or erasing crucial information so that representation of key aspects of the item does not occur, or produces an incorrect result.
	Dazzling	Obscuring or blurring information about the deception core, without eliminating it.
	Decoying	Distracting *threat agents'* attention away from what is really going on.
Showing the false: Actively include faulty representations of the deception core, i.e., *the criminal and his/her crimes.*	Mimicking	Assuming somebody else's identity or modifying the core so it copies the features of a legitimate item.
	Inventing	Making up information about the core. The core might not exist, or its characteristics might be utterly unrealistic.
	Relabeling	Describing the core and its characteristics in a questionably favorable way, expressly to mislead.
	Double play	Convincing *threat agents* that they are taking advantage of the deceiver.

Table 6.3: Deception tactics as proposed by [463, p.472], and refined by [470, p.198]. Terminology is further added from literature (*Hiding the real* and *Showing the false* [475]), and made more explicit based on the findings of this study: *deception core* and *core* are specified as *the criminal and his/her crimes*, and *victim* is replaced by the term *threat agents*.

Deception for deviant security purposes Deception tactics are also deployed for the main purpose of being a deviant security control. In such situations, deceptive practices are necessary for the cyber criminal not because of sexual, financial or other reasons, but primarily for security purposes. Again, cyber criminals have to hide the real and show the false. If the Ponmocup malware discovered that it was being analyzed on a security researcher's machine, it delivered a fake payload. More precisely, the malware installed an easy to detect and remove adware in a more obvious manner than the real payload [391, p.32]. Encountered deceptive security tactics in this study are offensive and defensive (such as honeypots), aimed at all threat agents, and of an administrative, physical and technical nature. Table 6.4 further shows that deceptive security mechanisms not only have deterrent, detective and preventive [470, pp.201-203][476, pp.101-102], but also corrective security functionalities.

Deception is truly the Swiss army knife of DevSec controls because of its multitude of functions, flexibility, user-friendliness and low operating costs. For instance, CSAM users generally have to deceive their immediate physical social surroundings about their sexual preference for years in a row. An admin of a cyber criminal forum was observed who posed as a legitimate security consultant, called his malicious forum 'a leading security platform', and spoke on major information security conferences. News media may also play a role by relabelling cyber criminals and their crimes as patriotic by linking cyber crimes to e.g., internal and external political conflicts [477, pp.235-246]; as corrective acts in which cyber criminals are apparently modern Robin Hoods who steal from the rich and give to the poor [478]; or as generally harm and victimless acts conducted by creative nerds while having their own legitimate magazine that explains how to commit cyber crime [479]. Moreover, accidents, failures and mistakes of cyber criminals may not only create disinformation [158, pp.131-132], but are sometimes also patched by deception tactics as shown by the masking example in Table 6.4.

Cyber criminal flocks
Cyber criminal groups may also improve the security of individual members because security is a club good in certain communities. Large flocks of cyber criminals work as a deceptive countermeasure as the share number of targets may dazzle cyber security communities (see *Data maximization* in Table 6.4). Several Chinese cyber criminal fora have near a million members. Target prioritization may therefore be a challenge for Chinese LEA. Similarly, the Russian-language underground might also be too large for the Russian cyber security community to handle. Moreover, the larger cyber criminal flock is safe when law-enforcement is investigating and prosecuting a single individual member and/or organized group behind botnets like Avalanche and Zeus: a labour-intensive process which may keep LEA busy for years. Flocks do also work for non-human entities. Placing your botnet C&C in a hosting country like the Netherlands underlines the same idea. As experienced during this study, there is simply too much badness on servers in the Netherlands for Dutch LEA to send official takedown requests to ISPs, let alone to preserve all the data on these servers, while ISPs might have incentives not to respond to abuse notifications of other key players [166]. Similarly, some online money launderers were observed who make large pools of transactions from which clients can deposit and withdraw cryptocurrencies, while carders mix large amounts of credit card credentials from various successful point of sale attacks. Such deceptive actions provide confidentiality and affect integrity. More specifically, these tactics respectively provide anonymity and unlinkability, and affect authenticity and non-repudiation which as a consequence protect the criminal (e.g., financial traces that lead to the identification of a suspect) and/or his/her crimes (stolen credit card accounts that are blocked by financial institutions).

It further becomes evident that well-described techniques in computer science such as obfuscation, spoofing and steganography are all deceptive security controls. Nota bene, encryption is not based on deception, but on the tactic of *denial*: overtly concealing communication, but not its existence [467, p.28]. However, encryption and its antithesis of secure-deletion (see Section 7.1) can be combined with deception to create *technical plausible deniability* about information assets (also known as content deniability [36, p.442]), more specifically hidden volumes in encrypted storages mixed with deletion passwords that wipe encryption keys [480].

Deviant security through deception	**Tactic**	**Control type and functionality**	**Observed practices**
Hiding the real - Prevent an accurate understanding of the criminal's identity and his/her actions.	Masking	Administrative correction	After registering one of his very first domains for a C&C with his true credentials, a botnet herder re-registered the domain using false credentials.
		Technical prevention	Visitors are shown legitimate content when they access a CSAM site without using Tor.
	Dazzling	Administrative deterrent	Data maximization (also known as data pooling [132, pp.2-3]) - Creating a hay pile, or connecting to an existing hay pile of data (i.e., noise), to hide an important needle (read: asset), such as deploying domain generation algorithms for botnets, or having a very generic or widely used nickname (e.g., 'money' or 'hack3r').
		Technical deterrent	Obfuscation - Malware developers obfuscate their code in such a way that their personal writing style will not be recognized [481].
	Decoying	Technical detection	Admins of a cyber criminal forum use a honeypot to attract, and subsequently detect, threat agents.
		Technical prevention	Steganography - Cyber criminals use misleading data carriers to hide the existence of communications and avoid detection, such as information hiding–capable malware [482][467, p.28].
Showing the false - Actively include faulty representations of the criminal's identity and his/her actions.	Mimicking	Administrative deterrent	A bulletproof hoster poses as a legitimate Internet service provider, and/or accepts legitimate customers.
		Technical prevention	Malware mimics sleeping on an infected machine for an extended period of time to avoid detection by a sandbox.
		Technical deterrent	Imitation - A malware developer attempts to write a code such that his/her writing style will be recognized as that of another individual [481].
	Inventing	Administrative prevention	Disinformation and lies - A member of a cyber criminal forum falsely accuses another member of being an LEA informant. Sending a copy of a false passport to a virtual currency processor as verification.
	Relabeling	Administrative correction	The influencing of the public opinion about cyber crime by projecting a favorable image of criminal hackers in media ('modern Robin Hoods' and/or 'patriots'), and justifying and/or downplaying their actions.
	Double play	Physical detection	Cyber criminals deploy double informants to deceive law-enforcement.

Table 6.4: This table structures observed deception practices with protective side effects as well as those practices exclusively for security purposes.

Vulnerabilities in deviant deception countermeasures Although deception controls protect the identity and business assets of individuals, the related tactics have serious blowback effects to the well-being of the larger cyber criminal community as nobody knows which information is accurate. So, deception fuels a *tragedy of the commons* on the accuracy of deviant security-related information in the cyber criminal community. Every individual applies deception according to his/her own self-interest, but contrary to the common good of all users by depleting the accuracy of information. This tragedy cannot be avoided by cyber criminals as its root cause lies in *inherent weaknesses* of deviant deception controls. As described previously, cyber criminals need deception for the successful commission of crime, and cannot always rely on other types of attacks that would create less information asymmetries. In other words, avoiding deception attacks with protective side effects implies that cyber criminals would paradoxically have to stop committing crime. The same line of reasoning can be extended to the use of deceptive tactics solely for deviant security purposes. Deception is a necessary stepping stone to successfully implement a range of other security measures, such as the use of a Trojan to install a RAT for monitoring co-conspirers. In other words, without deception, a range of vital deviant security countermeasures will be out of reach.

Similarly, because potential clients may lie about their true intentions - thus know more about future actions than the transaction partner, i.e., *hidden information* - it is hard for DevSec providers to avoid *adverse selection* prior to a transaction. BPHs, who are specialists in deception, might be deceived themselves by their clients who use rented servers for hosting CSAM or terrorist related activities, albeit forbidden by the BPH. So, deception works as a *feedback loop* that brings some of the costs imposed to the cyber security community back to the cyber criminal community that caused them.

Another vulnerability of many deception tactics is *security through obscurity* [59, p.34]: the false assumption that threat agents will not find the hidden real. Obfuscated information capital such as malicious code can be reverse engineered by security researchers. House searches by law-enforcement agencies hold the same effect: they are legally permitted to look for hidden physical assets such as cash money. Still, security through obscurity reduces the adversaries' rewards and/or increases the efforts of their threat agents [317, pp.279, 282], thus works as an effective delaying tactic.

Lastly, effective deception tactics should only target those threat agents that have the power to negatively affect the deceiver's assets. However, deceptive countermeasures cannot be deployed against a single type of threat agent. They target all possible threat agents indiscriminately with detrimental effects such as harming criminal business relations. As a result, security through deception fuels the need to install other deviant security measures. The next sections show that cyber criminals weapon themselves against deception attacks and information asymmetries by deploying not only trust mechanisms, but also countermeasures that rely on the opposite side of the coin: distrust mechanisms.

6.6 Trust and Distrust as Deviant Security Controls

How do cyber criminals patch the information asymmetries that are caused by deception tactics of key players? Much has been written about dealing with an underground economy riddled with dishonesty with online trust (as compared to offline trust in cyber criminal networks [196, pp.7-8]) [186, p.42][483][452][202]. However, no studies have been found that research online trust mechanisms from a deviant security perspective, thus as a countermeasure. At the same time, many cyber criminals do not solely rely on trust policies and mechanisms. On the contrary, there are good reasons not to trust your (potential) business partners at all. This section further shows that distrust is very much a deviant countermeasure, yet academically neglected.

Trust as a deviant security policy Trust is an intangible asset [381, p.6], and defined in terms of confident positive expectations regarding another's conduct (i.e., words, actions and decisions) [484, pp.439-440]. From a deviant security perspective, trust is a peer-produced club good [354, p.17], and about the referent object's expectations that a transaction partner is *not* a threat agent who threatens his/her assets. So each referent object autonomously assigns trust to a transaction partner at his/her own discretion [64, p.49]. Trust mechanisms generally follow the information asymmetries of person-to-person ('should I trust this person?'), person-to-system ('should I trust this system?') and system-to-system ('should my system trust this system?') [485]. Although system-to-system trust mechanisms do exist in botnets (see caption below Figure 6.7), observed deviant trust mechanisms are predominantly person-to-person and too a lesser extent person-to-system. This is explained by the idea that DevSec is neither a product specifically designed for the criminal market, nor regulated by law. The underground economy has not developed system-to-system trust controls. Cyber criminals do not have their own certificate authorities (CAs) that provide system-to-system trust by issuing public key infrastructures. In fact, cyber criminals must rely on regular CAs for their security when they apply SSL for e.g., their fora. The absence of law rather paves the way for personal qualified trust providers. These facilitators operate on a decentralized person-to-person level, such as the previously mentioned malafide escrow services (nota bene, the exchange of trust for money in the form of a service converts the intangible to a tangible asset). So, cyber criminals have no other option than merely raising the issue of the trustworthiness of a particular *system* on a cyber criminal forum, and discussing whether or not trust that system. No matter how advanced these trust mechanism are - ranging from a mere discussion, whitelists or advanced procedures as described in the next paragraph - the outcome is that the actor or system involved ranges from *trusted* to *not trusted*, and receives a corresponding *security clearance* (see Figure 6.7).

Deviant trust mechanisms Trust as a deviant security control builds upon the research on decentralized person-to-person trust mechanisms of netizens (Johnson, Crawford and Palfrey [354]) and cyber criminals (Holt and co-authors [197][453], Lusthaus [202], and Yip, Webber and Shadbolt [452]). Based on the findings of this study, adjustments are made to the conceptual understanding, structural order and terminology of trust mechanisms as security controls, most importantly by aligning trust to attribution (establishing and subsequently trusting *who* and *what* of a potential business partner). As depicted in Figure 6.6, assigning deviant trust is an *authentication* process that consists of three successive steps:

1. *Establishing cyber criminal identity (who).* The first step is to establish the criminal nature of the potential collaborator - read: confirm or reject his/her criminal identity - which consists of e.g.,:

    - Background checks [202][454, p.44]: Review of information related to the business partner's identity on closed and open sources, including member status within cyber criminal community [200, pp.43-44]; and
    - Criminal acts as signals and information hostages [453][202]: Review of and/or requests for incriminating evidence about current or past cyber crimes such as mandatory uploads of CSAM or stolen credit card credentials.

    These controls are especially effective against mandated breachers. Pseudo-purchases by police officers are evasive investigative powers which are not easily allowed by prosecutors and/or investigative judges, and might sometimes even be impossible in some jurisdictions, such as uploading child abuse images to gain access to closed CSAM fora.

2. *Establishing criminal conduct/outcomes (what).* Once the criminal identity of the potential business partner is confirmed, the cyber criminal has to assess the past and present conduct and produced fruits of his/her future associate. He/she might ask and/or be given proof of past and current crimes, such as screenshots of previous payments or samples of compromised credit cards, similar to the previously described criminal acts as signals. However, without prior businesses experiences, the cyber criminal further has to rely on e.g.,:

    - Referrals [202]: Recommendations by other cyber criminals on which reputation is build [431], including positive reviews via public threads on fora and mouth-to-mouth referrals via private chat messages; and

    - Prowess demonstration [202]: Examination of an individual's human and information capital, which includes reviewing and testing products and services [197, p.166].

These first two mechanisms underline what DevSec is: an asset that protect assets. Referrals and prowess demonstration give information about intangible assets of the cyber criminal, such as his/her information, human and organization capital. This does not only relate to the future partner's ability to commit crime, but also his/her ability to *protect* his/her own and his/her counterpart's identity and activities. In a reviewed interview transcript, a convicted person with a well-developed technical skill set and well-established reputation in the underground economy stated that he would not trust individuals that do not use the cryptographic protocol Off-the-Record Messaging (OTR) during instant messaging conversations as this person probably lacks human capital on technical computer security and therefore poses a vulnerability. So a cyber criminal has to assess whether he/she can trust his/her potential partner and related business, and if that individual does not pose a vulnerability to his/her own identity and/or business operations. If the criminal identity and business are sufficiently confirmed, the cyber criminal has to make a decision: is the potential partner to be *trusted* to make a deal? If not, he/she might still proceed with the transaction by making use of escrow services.

Viewed from a DevSec perspective with its emphasis on the protection of crime and the criminal, these first two steps of the authentication process are of a *preventive* nature about trusting the *what* and *who* of a transaction partner. By assessing the identity, conduct and outcomes of the potential partner, the cyber criminal hopes to prevent damage to his/her own identity and business. If the business partner is trusted, they may stick together for many years. A Russian-language job scam service, for instance, rented servers from a reliable bulletproof hoster for over four years until the money launderer was arrested by LEA. While the previous steps result in the decision that a partner is trusted, that is not to say he/she is also *trustworthy* [36, pp.9-10][285]. Similar to CAV services, credit card checkers test whether stolen credit cards have already been blocked by financial institutions. Yet some of these underground enterprises that offer their service to carders for free, secretly log the test results and use the validated credit card numbers for their own gain before their customers can [409, p.7]. In other words, although they are trusted by carders who upload their stolen credit cards, these DevSec-as-a-service providers are not trustworthy as their clients are unaware of the *customer data monetization* behind this *free business model*. Therefore, the last step consists of:

3. *Enforcing trustworthiness through extra-legal governance* [202][454]. Mechanisms that enforce trustworthiness are of a *corrective* nature as these mechanisms try to correct undesirable events that have occurred. Because cyber criminals can generally not rely on centralized governance (e.g., states) when trust is betrayed [453, p.1], peer-produced security in the form of extra-legal governance is needed by the community itself. Escrow services provide qualified trust services, and cyber criminal fora allow naming and shaming of scammers and rippers, even banning untrustworthy members and/or deleting their posts [368, p.7][266, p.6]. Negative recommendations ('a trusted partner was untrustworthy') and positive

> recommendations ('a trusted partner was trustworthy') affect the reputation of the transaction partner, and subsequently provide input for the first two steps of the authentication process of other cyber criminals. Thus decentralized decisions about about who and what to trust will increase the security as a common good for the larger cyber criminal community [354, p.17]. Other corrective controls are discussed at the end of this section.

Vulnerabilities in deviant trust countermeasures A first weakness of trust controls has already been touched upon in the previous paragraph. Research on trust in a cyber criminal context, most notably [202][452], focuses very much on the cyber criminal's assessment of his/her counterpart's tangible and intangible assets that relate to his/her business partner's *commission* of crime and identity. But besides the cyber criminal's decision that his/her counterpart is criminal and able to commit crime, the cyber criminal also has to assess whether his/her co-conspirer is able to *protect* the criminal's and the co-conspirer's own identity and malafide business. Indeed, not only academics overlook this assessment, but criminals as well. A cyber criminal was observed who needed several critical services from another criminal to conduct online scams. However, the real offline identity of this service provider was very easy to discover on open Internet sources, which increased the chance that LEA would intervene.

Another fundamental flaw - read: inherent weakness - in these trust mechanisms is *trusting trust*. Trust is very much an assumption [64, p.50], and no amount of verification or scrutiny will protect a cyber criminal from collaborating with untrustworthy persons or systems [486]. In theory, each transaction partner should autonomously assign deviant trust at their own discretion, and be able to verify the trustworthiness of the other business partner [64, p.49]. However, this is not always possible in the cyber criminal underground. This vulnerability is most apparent by the middlemen that launder virtual dirty money for cyber criminals [487]. Besides theft by malicious Bitcoin tumblers [403], the exit scams of the Evolution cryptomarket and Mt. Gox cryptocurrency exchange - essentially, qualified trust providers - are great examples of trusted third parties for cyber criminals that were, ultimately and just a single time, not trustworthy [488]. It has been suggested that even the fundraisers set up by angry customers to sponsor doxing campaigns against the persons behinds the exit scams were scams as well [489]. So, trusting trust promotes *perverse economic incentives* for transaction parties in the cyber criminal underground to take decisions that negatively affect the other parties involved.

Moreover, trust mechanisms protect the business between transaction partners from attacks by other cyber criminals like rippers, but do not protect identity against attacks from law-enforcement. On the contrary, trust mechanisms may pose an inherent weakness to the protection of identity. In order to establish and sustain a reputation and trust of transaction partners, individuals may share personal identifying information to one another. However, the exchange of personal information may also hold blowback effects as gener-

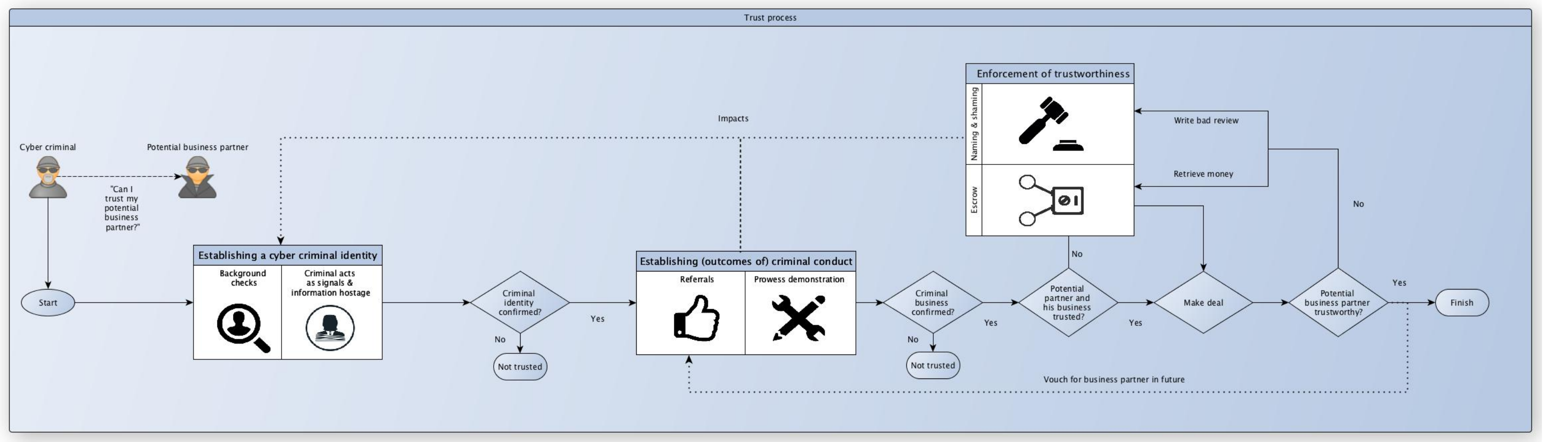

Trust process
Cyber criminal
Potential business partner
"Can I trust my potential business partner?"
Start
Establishing a cyber criminal identity
Background checks
Criminal acts as signals & information hostage
Criminal identity confirmed?
No
Not trusted
Yes
Impacts
Establishing (outcomes of) criminal conduct
Referrals
Prowess demonstration
Criminal business confirmed?
No
Not trusted
Yes
Enforcement of trustworthiness
Naming & shaming
Escrow
Write bad review
Retrieve money
No
Potential partner and his business trusted?
Yes
Make deal
Potential business partner trustworthy?
No
Yes
Finish
Vouch for business partner in future

Figure 6.6: Three steps in deviant trust: establishment of criminal identity, establishment of criminal conduct and enforcement of trustworthiness.

ating such information might help attribution by threat agents. Indeed, Dutch court cases show that some CSAM users exchange a lot of personal information and incriminating evidence with trusted like-minded others [139]. Similarly, advanced computer-focused criminals were observed who discussed their private lives with trusted partners during chat conversations over trusted lines.

Lastly, trust has obvious reputation benefits for cyber criminals as a respected nickname indeed works as a trusted brand which generates new transactions between individuals who have had no prior knowledge or experience with each other [452, p.526][202, pp.80-81]. The downside of a well-established trusted identity - read: *reputation cost* - is that it will attract the attention of threat agents, most notably mandated breachers. Law-enforcement agencies prioritize their proactive investigations on - amongst others - the reputation of cyber criminals, a problem which trust mechanisms cannot overcome, but actually create. Assets that are considered competitive advantages for legitimate businesses might well be *competitive disadvantages* for cyber criminals. Being a trusted and well-known brand, having automated processes and the ability to scale, offering high-quality products/services and features such as 24/7 support does not only attract many customers and high revenues in the underground economy [267, pp.170-174]. It will also draw the attention of threat agents that do not want to enter the competition but will use all necessary means to take the criminal out of business permanently. Thus, *dynamic interplay* on security spending between referent objects - 'I installed better security mechanisms than my competitors, and therefore I am safe against threat agents' [81, p.12] - is not applicable in the underground economy. Cyber crime units of federal and national law-enforcement agencies - most notably, the American FBI and United States Secret Service (USSS), the British National Crime Agency (NCA) and German *Bundeskriminalamt* (BKA) - do not prioritize their targets on the degree and kind of deviant security and related weaknesses, but on the success level of committing cyber crime and financial damage to the cyber security community, most notably victims.

Distrust as a deviant security policy Trust in general should be justified, and the referent object must have the opportunity to autonomously verify the trustworthiness and control the actual behavior of his (transaction) partners [64, p.49]. To do so, cyber criminals may install distrust mechanisms. As depicted in Figure 6.7, trust and distrust are separate and distinct constructs and not opposite ends of a single continuum [484, pp.439-440][490]. Similar to bonafide environments [484, pp.448-449][491, p.29], both policies may well coexist in malafide environments. This explains why cyber criminals simultaneously deploy distrust mechanisms before, during and after the previously described three steps of the trust process when operating on the cyber criminal market and/or collaborate with co-conspirers. The security policy is: trust but distrust. This indeed a variation on the Russian proverb 'доверяй, но проверяй' ('doveryay, no proveryay'): trust but verify. As observed during this study, members of Russian-language cyber criminal fora actually used this proverb to discuss e.g., the degree of anonymity of VPNs and spyware. The simultaneous coexistence of trust and distrust mechanisms ensures a *compensating* layer of security, thus an alternative control that provides similar protection as the original control. This further shows that cyber criminals want to minimize *ex-post losses* due to attacks by non-trusted and distrusted actors, by not only relying on *ex-ante* trust mechanisms but also simultaneously invest in *ex-ante* distrust controls.

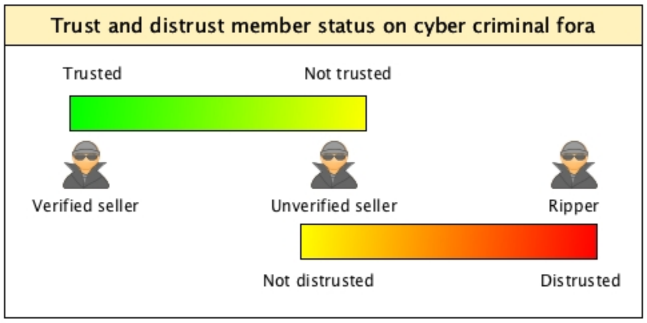


Figure 6.7: The official status of CaaS forum members may relate to trust and distrust. Some vendors are labelled as verified sellers. Buyers have positive expectations regarding the seller's conduct. They are trusted and therefore on a *whitelist*. Rippers are distrusted, and for this reason on a *blacklist*. Buyers have negative expectations about their conduct. Those who have the status unverified sellers on a forum are not on the whitelist, nor on the blacklist: they are not trusted, but also not distrusted. In other words, buyers have neither negative, nor positive expectations about these vendors. Be aware that whitelisting and blacklisting is not only deployed as a person-to-person mechanism but also system-to-system in e.g., p2p botnets. The GameOver Zeus botnet applied blacklists of IPs of crawlers and sensors of the cyber security community to prevent bots from communicating with them. The Sality botnet used a reputation system based on a goodcount, which reflects how well-behaved peers have been in the past. The result of the latter system-to-system trust mechanism is that sensors were only propagated to other bots if they had achieved a positive goodcount, thus positive expectations about connecting to this peer. This reputation scheme worked against infiltration attacks from the cyber security community [158, p.131][492].

Opposite to the former trust definition, distrust is defined in terms of confident *negative* expectations regarding another's conduct [484, pp.439-440]. In other words, the referent object expects that an actor might be a threat agent that threatens his/her identity or malicious business operations. Distrust in general is expressed by wariness, skepticism, and behaviors as defensiveness, watchfulness, and vigilance [484, p.446][284]. The outcome of this policy in a deviant security context is that the actor involved is regarded in a range from *distrusted* to *not distrusted*, and receives a corresponding *ban* (as compared to a clearance).

Both distrust and trust protect business operations. Only distrust, however, protects identity as well, while trust mechanisms do not (see Table 6.5). On the contrary, trust provides security for all parties concerned with each party having their own protection interests and goals. This form of multilateral security is based on exchange of information about each other's identity which reinforces the bond between co-conspirers. This smoothens business operations but poses a vulnerability that the true identity of a cyber criminal will be revealed when e.g., communications are intercepted or a criminal colleague is apprehended. Distrust is unilaterally enforced, limits the autonomy of the distrusted party over his/her own security, and prevents the distribution of sensitive data assets. Cyber criminals have good reason to apply distrust: a *false positive* - a trusted business partner is not trustworthy - holds a major impact for the safe-being of their business and identity.

Countermeasures	Identity protection	Business protection
Distrust	✓	✓
Trust	✕	✓

Table 6.5: Because trust only protects malafide business, cyber criminals simultaneously apply distrust mechanisms to control the protection of identity as well.

Deviant distrust mechanisms Most observed distrust mechanisms are of a predominantly *preventive*, *detective* and *deterrent* nature (see Table 6.6). These mechanisms can be categorized as follows:

- Preventive controls:

  Compartmentalization (or compartmentation): Cyber criminals isolate data, software and hardware within different compartments (like a virtual machine solely used to collect CSAM), or organizational cells within larger collaborations (e.g., forum admins may only share some of their deviant security mechanisms with each other, and not with members of a lower status). As such, *confidentiality* is achieved via these respectively rule-based and role-based controls. The isolation of information is closely related to *internal secrecy*: keeping information from insiders - i.e., co-conspirers, forum members and so on - because of distrust. Internal secrecy differs from the many examples in this study of external secrecy: keeping information from outsiders which may actually promote trust between insiders [493, pp.29-30]. The group behind the Tyupkin malware generated a unique digit combination key based on random numbers for every ATM attack. This ensured external secrecy as no person outside the group could accidentally profit from the fraud. The hacker that physically operated near the ATM then received instructions by phone from another group member who knows the algorithm and is able to generate a session key [494]. This internal secrecy policy (i.e., person-to-person) subsequently ensure that the hacker who also collects the cash cannot act on his/her own.

  Data-minimization: A common security policy for confidentiality, more specifically *anonymity* and *unlinkability* [207, p.6], is to minimize the amount of content and metadata related to respectively the criminal and crime, such as botnets that return only a small set of peer list entries (i.e., system-to-system) [158, p.131]. A piece of advice which is frequently posted on cyber criminal fora is not to reveal any personal details during communications. Lawful intercept shows that some cyber criminals strictly apply this policy, while others disable logging. They distrust the technical line of communications, as well as their business partners and systems (i.e., person-to-system).

Regulations: Bureaucratic and regulatory controls are also based on distrust as they increase control [484, p.446][490, p.885]. Besides informal norms and unwritten rules, many cyber criminal fora have access rules [454, pp.39-40], and terms and conditions with do's and don'ts. An exclusive, paid membership Russian-language forum had, for example, over 40 rules. Admins and their helpers - official moderators, snitches and unofficial watchdogs - heavily enforce these rules by moderating the threads and postings of members.

– Detective controls:

  Investigations: Investigations by cyber criminals are very much a security measure [59], yet of an offensive nature. These investigations are launched because of suspicion, which is synonymous for distrust [491, p.41][284, pp.587-590]. These investigations aim at detecting undesirable events that have occurred and *accountability* of those responsible for failures, mistakes and deliberate attacks. Investigations are frequently deployed on fora to find duplicate identities, but are also launched after exit scams, rip deals and DDoS attacks.

– Controls of a preventive *and* detective nature:

  Labelling: Covert and overt labels of cyber criminals to (potential) threat agents may also point to distrust when these are signs of limiting influence of, or not granting authority to others [491, p.44]. Observed covert labels are silent alarms on cyber criminal platforms. Forum admins had negative expectations towards their members regarding screenshot leakage. They secretly watermarked each user account with an unique graphic display for detection purposes [495]. Examples of overt labelling are admins who give members limited privileges or a distrusted status like ripper.

  Testing: Tests are means by which the presence, quality and/or genuineness of objects and subjects are established by cyber criminals because of potential negative expectations. Human-to-system distrust mechanisms are counter-antivirus services ('should I distrust my malware?'). When such a testing service reports to a crypter that his/her obfuscated malware is detected by antivirus products, the criminal is sure to distrust the malware sample. If the service reports no hits that is not to say that the malware should be trusted. CAV services produce *false negatives*, and the underground community is well aware of this problem. Cyber criminals frequently test malware against a range of CAVs to prove that these malicious services produce different outcomes, and subsequently publish these results on fora.

Malware says no
Advanced malware frequently has system-to-system distrust functionalities ('should my system [read: malware] distrust this system?') as it conducts a range of tests to make sure that the system is not controlled by a security researcher. A reviewed ransomware assessed the number of stored files on computer systems. If there were less than twenty files, the computer was likely a security researcher's honey pot. Rombertik malware 'slept' (read: was inactive) for a while to fool sandboxes, and also checked if it was not analyzed in memory. The malware further examined if analysis tools modified the code by sending invalid arguments and only accepting a specific error as compared to a general error from sandboxes that suppress specific errors. Rombertik would also check the username and filename of the executing process for strings associated with security researchers like 'malwar', 'sampl', 'viru' and 'sandb' [336]. In other words, the malware checked its own integrity prior, during and after installation. The Cobalt/Buhtrap malware checked if time and date of the victim's system was congruent with a clock functionality in the malware [496]. Lastly, SpyEye malware would test a victim's system if it was already infected with the competing Zeus malware and subsequently removed the competing malware [497]. Similarly, Netsky malware tested systems on Beagle and Mydoom malwares [498].

– Controls of a deterrent *and* detective nature:

  Monitoring: Similar to regulations, monitoring - including surveillance, supervisory controls and logging - is related to distrust as it aims at increasing control [491, p.44][490, p.885]. Monitoring allows the detection of suspicious traffic and/or behavior, and as such promotes two attributes of integrity namely *accountability* and *auditability* [27, p.12][32, p.159]. While some suspects minimize the amount of data they generate, others log metadata of incoming-outgoing server traffic and written communications with e.g., co-conspirers (sometimes even adding notes with personal observations to the logs). More offensive countermeasures were observed within a very hierarchal cyber criminal organization. The leaders secretly installed RATs on the computers of co-conspirers as a detection control to technically monitor them and their activities, but also promoted a manual reporting mechanism among lower tier members for the same purpose. An example of physical surveillance/supervisory controls of a more deterrent nature are moneymules that were escorted and observed by moneymule managers whom used professional counter-surveillance tactics. Cyber criminal fora also monitor members' activities with the help of administrators/moderators, forum bots and the larger community [368, p.5].

Distrust controls	Preventive	Detective	Deterrent
Compartmentalization	✓		
Data-minimization	✓		
Regulations	✓		
Labelling	✓	✓	
Testing	✓	✓	
Investigations		✓	
Monitoring		✓	✓

Table 6.6: The various security categories of distrust controls. Notably, sanctions for being distrusted - such as exclusion - are corrective controls, while distrust itself is a compensating control to trust mechanisms.

Vulnerabilities in deviant distrust countermeasures Deviant distrust mechanisms show that cyber criminals face two (related) tradeoffs. The first is *efficiency versus effectiveness,* more specifically *complexity versus accuracy.* Forum members expect that investigation, prosecution and verdict are conducted as soon as possible by admins and their helpers, i.e., the trias politicus (see Section 5.4). This requires efficient, thus cheap, simple and fast investigations. However, the outcomes might be not that effective as they are more prone to error (i.e., not accurate). If the outcomes of applying distrust mechanisms lead to too many false positives - cyber criminals are unjustly distrusted - and punished, the conversion rate of successful transactions decreases. In such situations, cyber criminals miss out on potential revenues because of failed transactions. Worse, false positives work as an amplifier for even more distrust in the cyber criminal community. Investigations by cyber criminals do not follow an evidence standard of beyond reasonable doubt. Let alone that there are trained defense attorneys and independent judges in the underground. These investigations will likely produce incorrect conclusions about the truth ('who did what?'), and as a result create disinformation. This shows that cyber criminals have to strike a balance in distrust and trust mechanisms between the *false accept rate* (fraud rate) and *false reject rate* (insult rate). So, they face a second tradeoff, namely reducing false positives by decreasing deviant security standards, versus reducing false negatives by increasing these standards.

Even if the distrust mechanisms produce the desired outcomes, they may hold negative side-effects and vulnerabilities. Compartmentalization, bureaucratic rules, data-minimization and monitoring place a burden on the efficiency of committing cyber crime and may even devalue a criminal product or service. Many BPHs forbid certain illegal activities on their servers which decreases the prospect of attracting new customers. Furthermore, audit logging and subsequently saving that data on application level (i.e., local storage on a laptop) will pose a danger when LEA is able to seize that data, e.g., after a house search. Cyber criminals who apply bureaucratic rules, compartmentalization and data-minimization face an insurmountable problem that further negatively affects the effectiveness of these distrust mechanisms: those who do not obey these rules.

In many of the reviewed cases, important personal identifiers are revealed by others. Some ask in online communications such questions as 'How was your vacation in [name country]?' to 'How are your kid [name X] and wife [name Y] doing?'. Remarks like 'Happy birth day!' to 'I spoke to your mother the other day' have also been observed. Lastly, distrust further fuels information asymmetries in intertwined networks. Distrust leads to *information distortion* [491, p.44], while compartmentalization and data-minimization specifically limit the amount of information to make informed decisions about deviant security.

Corrective controls in trust and distrust mechanisms While trust mechanisms consist of three consecutive steps ending with the corrective control of extra-legal governance, distrust mechanisms are less connected and ordered in a linear fashion. Prevention and/or detection controls warn cyber criminals about imminent threats or actual attacks, and are followed up by investigations that are launched by cyber criminals. In the labelling example, a screenshot of the forum was indeed leaked by an investigative journalist on the open Internet. The admins launched an investigation to establish which user account was compromised, and subsequently applied a *corrective* control: they banned the user of the account from the forum (see also [454, pp.43-44]). Such forum bans can be temporary or permanent. On some fora, members with enough negative points are automatically banned [368, p.7]. Alternatively, warnings, fines and restitution orders are given, including lowering the numeric or status reputation of a member. Some forum admins share information about banned members, thus provide DevSec as a club good to a larger cyber criminal community and avoid *coordination failure*. Notably, not transacting business has been called the 'ultimate weapon of the [...] distrustor' as this financial punishment (as compared to physical and psychological violence as punishments, see Section 7.4) leads to *unproductive isolation* [490, p.885][64, p.49]. Other observed corrective controls of cyber criminals include doxing and seizure of cryptocurrency assets. These (threats of) punishments promote trust and distrust mechanisms and help to sustain cooperation in cyber criminal networks [115, p.1048]. Be aware that the malware in the distrust testing example also applied a corrective control. If there were positive results, such as detection of a researcher's sandbox or a competitor's malware, the malicious software respectively removed itself or the competing malware from the victim's system. Thus, besides many *ex-ante costs* to prevent, deter and detect attacks, failures and mistakes, cyber criminals also make *ex-post costs* to correct, recover and restore security violations. Be aware that cyber criminals may also have negative expectations about the outcomes of their own actions. Because referent objects are autonomous, they may choose to correct themselves, and withdraw from the commission of crime during the preparation, pre-activity, activity and post-activity phase. An example of such a self-corrective control in the post-activity phase is the operators behind the Crysis and TeslaCrypt ransomware who released the master keys to victims to decrypt and unlock infected systems for free [499][500]. A last observation is that these corrective controls generally focus on securing crime, namely: the protection of criminal business processes, products and services. Only a few corrective controls have been observed that protect the criminal's identity. Besides offensive countermeasures such as bribery and violence (see e.g., [364, p.6]), there is simply little suspects can do when personal data is in hands of threat agents.

6.7 Interim Conclusion and Discussion

The purpose of this chapter was to describe the key players of deviant security and their security-related interactions including associated countermeasures. Many of the related vulnerabilities are explained in microeconomic terms such as allocation problems, feedback loops, lemon markets and perverse incentives, and tradeoffs as efficiency versus effectiveness, complexity versus accuracy and false accept rate versus false reject rate. Because everybody can instantly become a threat agent, the overall findings of this chapter suggest that cyber criminals need the ability to protect anything, *against anybody* which adds to the complexity of conducting an accurate deviant risk assessment. This insight holds significant implications for understanding how law-enforcement agencies can deal with the key players of deviant security, their security-related interactions and associated deviant countermeasures. These appropriate responses are discussed in Chapter 8.

On referent objects, providers and threat agents of DevSec The results of this study indicate that referent objects as a collective are to a certain extent autarkic, and as individuals autonomous, in formulating DevSec policies and subsequently implementing them. More research is needed to understand how and when cyber criminals become increasingly autonomous in their security. Thus besides an agenda for longitudinal studies how the cyber criminal's career path progresses in the commission of crime [345][215], research is equally needed to understand how cyber criminals - as communities, groups and individual referent objects - mature and become more autonomous in the protection of crime and the criminal. Another group of *key players* are providers of deviant security, and they can be distinguished between those who intentionally supply security to cyber criminals and those who unintentionally supply DevSec. The current study presents a simplified crime script analysis of the various services and products offered on the broader cyber-crime-as-a-service market. Future studies could use this model to plot the various services of individual fora, and see the similarities and differences between e.g., Chinese, English and Russian-language market places, or high-threat platforms with advanced computer-focused criminals and low-threat platforms with less skilled members. Another application is to make crime script analyses on a lower level of aggregation such as for different types of cyber crime. While studies have used linguistic-based empirical analysis on chat conversations of sexually-driven offenders to gain useful insights and patterns in the commission of online grooming [501], future work that applies a similar approach - e.g., using chat conservations of script kiddies behind DDoS attacks - should explicitly incorporate the protection of crime as well. Legal practitioners need to know who holds what role in a group and provided the necessary organizational, human and/or information capital, and tangible assets like payments, in the preparation, pre-activity, activity and/or post-activity phase of an attack. A last category of key players are threat agents to the security of cyber criminals. The research findings further provides evidence that besides bonafide parties - like mandated breachers - other key players can be threat agents to cyber criminals as well, including (victim) witnesses, security researchers, other criminals and the referent objects themselves. It is, however, unknown who the most important threat agent of cyber criminals is, both subjectively and objectively, and whether there are differences on this issue between computer-assisted and computer-focused criminals.

On intertwined networks & information asymmetries The study provided evidence that cyber security and cyber criminal networks are very much *intertwined* as different key players may hold multiple roles in time. Future studies, which take this insight into account, are needed to determine to which degree e.g., computer-assisted, computer-focused and computer-enabled communities are intertwined in the Russian-language underground economy [259, p.7], and on English-language cryptomarkets such as Alphabay. Do suppliers of computer-focused and computer-assisted crimes on these traditionally computer-enabled crime platforms form separate or intertwined communities? Do the former groups also buy products/services of the latter group, and vice versa? Do some individuals act as a community bridge between these groups, and why? Do cross cutting service providers (like online money launderers) or certain nationalities, play a vital role in socially linking individuals to one another, thereby decreasing the information asymmetry between other nodes in the network? There is, for example, anecdotical evidence of bilingual (i.e., Russian and Romanian-speaking) Moldovans who act as intermediaries between the Russian and Romanian-language underground economies. The present study further argues that *information asymmetries* in these intertwined networks not only exist between transaction partners, but that there are also information asymmetries for cyber criminals about third party threat agents that are not part of any transaction, such as law-enforcement agencies. There are still many unanswered questions how cyber criminals generally cope with these information asymmetries. How does corruption work in the cyber criminal underground, including the little understood обнал ('obnal') fraudulent encashment services and their clients - a reversed way of money laundering in which clean money is made dirty for bribery purposes [376][405] - that are offered on cyber criminal fora? Moreover, do cyber criminals with access to the security apparatus behave differently in e.g., their online communications? Better insights into the who, what, when and how of information flows through cyber criminal networks is also needed. One observation of this study is that very relevant information about capabilities and/or sources of law-enforcement agencies sometimes spread very slowly in cyber criminal networks, while irrelevant news about LEA in several occasions was discussed at great length and as such has the potential to become common sense yet useless knowledge.

On deception as a countermeasure One of the causes for information asymmetries in intertwined networks is the use of *deception.* This study demonstrates that hiding the real and showing the false is not only used to commit crime, but is also deployed exclusively for deviant security purposes. An existing taxonomy for law-abiding entities is adjusted to the deceiving practices of cyber criminals, and further refined by adding - amongst others - types and functionalities of technical computer security. The study concluded that deception has serious, but unavoidable, blowback effects for the larger cyber criminal community. In other words, commission and protection may hold inherent weaknesses which are inescapable for cyber criminals as compared to more optional vulnerabilities. In general, more work is needed on deception providers, such as suppliers of preconfigured VMs, fake IDs and hardware modification. Their services and products are vital for protection, yet it is unknown what their MOs are as they operate in the background of the cyber criminal value chain and thus have a low visibility for LEA. Future research might further explore if certain deception tactics are specifically tied to certain cyber crimes. Bulletproof hosting resellers and connectivity providers, for example, must pose as legitimate companies towards bonafide ISPs, thus heavily rely on mimicking, to ensure business continuity and avoid being rejected as clients. It might well be that other cyber crimes lean more towards alternative deception tactics.

On trust and distrust as countermeasures To overcome the problems associated with information asymmetries in intertwined networks like the previously mentioned deception tactics, cyber criminals deploy *trust* and *distrust* mechanisms. The key strength of the corresponding section is its usage of technical computer security concepts to understand the deviant security goals of trust and distrust mechanisms. A noteworthy contribution is made by regarding deviant trust as an authentication process that *ex-ante* assesses the criminal identity (*who*) and the (the outcomes of) criminal conduct (*what*), and *ex-post* enforces trustworthiness through extra-legal governance. As Section 7.2 describes, fora on the open Internet may have dysfunctional reputation systems as deals are closed and paid via other channels [454], while cryptomarkets heavily rely on reliable technical rating systems linked to actual payments to lower information asymmetries between buyer and seller. Bearing in mind two observed trends in cryptomarkets during this research project - i) the transform of Russian-language computer-focused fora into cryptomarkets, and ii) the entry of computer-focused and computer-assisted service providers to English-language computer-enabled cryptomarkets - future studies could focus on what impact these reliable technical reputation mechanisms have on the business transactions of intangible assets like stolen creditcards, malware and bulletproof domain registration. This is the first study that reports about distrust as a deviant security control. Based on empirical evidence, this study presents a taxonomy that consists of seven distrust tactics. Ultimately, the overall security policy 'trust but distrust' serves preventive, detective, deterrent, corrective and compensating technical computer security goals. Taking into account the many studies about trust in the cyber criminal underground, more work is required on distrust mechanisms. Generally, deception and distrust mechanisms are associated with more competitive environments, while trust policies are associated with more cooperative environments [363, pp.242-243]. Is this also true for cyber criminals? Are distrust mechanisms more prevalent in competitive profit-driven environments like the CaaS economy than in noncompetitive and nonprofit environments like sexually-driven CSAM platforms? Lastly, future work could also make a first step in exploring the unwritten rules and code of conduct of the Russian-language underground, and if there exist a cyber criminal variation on вор в законе ('vor v zakone' - thief in law).

Chapter 7

When & Where? - Temporal-Spatial Qualities of Deviant Security

Good guy security has spatial and temporal qualities. Not only because security has different meanings across and in time, but also because security only endures as long as the referent object is able to defend him/herself against attacks [31, pp.11, 18]. Yet we have seen in Chapter 5 that deviant security is a legal construct and a subjective condition, and will therefore have different meanings in time and space. The main question in this chapter is therefore: how do dimensions of time and space affect deviant security? Several scholars elaborated on how conceptions of time and space are altered in the Information Age, and the effects on the commission of cyber crime [34]. Because much of today's social, economical, cultural and political structures evolve around IT, new targets appear who experience the collapse of the temporal-spatial barriers [28]. Potential victims who are located anywhere in the world can be rapidly attacked in an automated fashion due to speedy Internet connections, from any location at any time [80, pp.80-81]. So, information technologies create new opportunities to commit crime because of the disappearance of time and space barriers that Castells respectively dubbed timeless time and space of flows (the latter is also known as placeless space) [45].

Since the commission of crime and the protection of crime and identity are inextricably linked, these temporal-spatial dimensions also affect deviant security. Scarce deviant security resources continuously change through time and place, and create controls and vulnerabilities alike that are discussed in the first section - see Figure 7.2 - about data volatility and retention as countermeasures. A common thread of this chapter is further the glocalised nature of DevSec. As shown in Figure 7.1 and Table 7.1, both global and local dimensions on a macro, meso and micro level impact the security of cyber criminals. More specifically, DevSec policies are based upon threat agents and threats in a specific local political, physical and/or social situation, and implemented by globally available security mechanisms. These dimensions are noticeable in the second and third section about two deviant temporal-spatial countermeasures, respectively intercultural communication between cyber criminals and the distribution of criminal assets. While the emphasis of the previous chapters has so far mostly been on administrative and technical controls, one might forget that cyber criminals are human beings who live in a physical world. The last section therefore moves from the online to the offline world, and discusses the physical countermeasures of cyber criminals on a micro level. So when time and space (*when* and *where*) are added to the *what* and *who* of the previous chapters, it becomes apparent that cyber criminals must be able to protect anything, against anybody, *anywhere, at any time.*

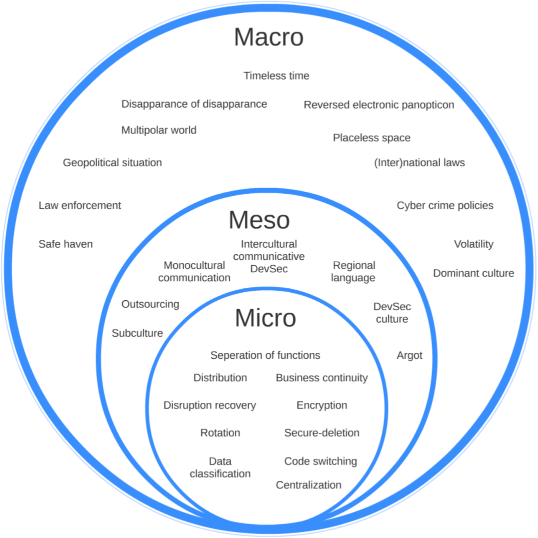


Figure 7.1: The conditional and consequential matrix presents some of the key concepts of this chapter that shape the glocalized nature of DevSec. Be aware that the term global does not equal to macro, and the term local to micro. Some deviant security policies are shaped by a local situation on a macro level (e.g., strong law-enforcement), and subsequently implemented on a micro level by globally available dual-use technologies (e.g., encryption), see Table 7.1.

DevSec levels	**Macro**	**Meso**	**Micro**
Local	National cyber laws	Rare regional language	Environmental design
Global	Multipolar world	Argot	Encryption

Table 7.1: Deviant security is shaped on different levels of aggregation. While a rare regional language is very local and argot has more global dimensions, both language-usages occur on the meso level of closed fora and chat groups.

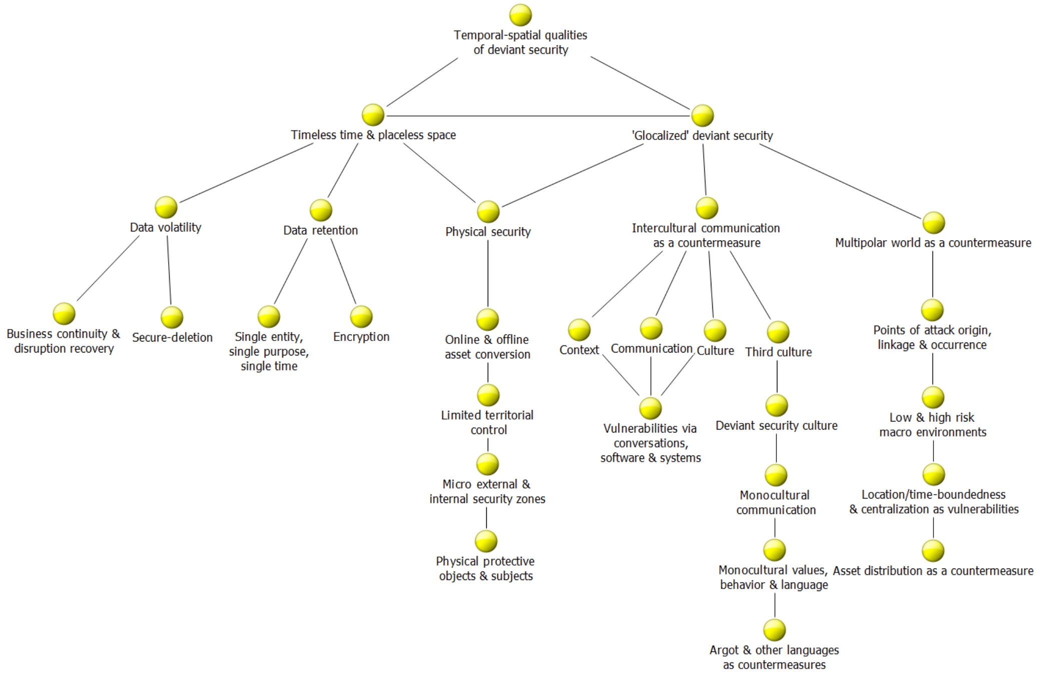

Temporal-spatial qualities of deviant security
Timeless time & placeless space
'Glocalized' deviant security
Data volatility
Data retention
Physical security
Intercultural communication as a countermeasure
Multipolar world as a countermeasure
Business continuity & disruption recovery
Secure-deletion
Single entity, single purpose, single time
Encryption
Online & offline asset conversion
Context
Communication
Culture
Third culture
Points of attack origin, linkage & occurrence
Limited territorial control
Vulnerabilities via conversations, software & systems
Deviant security culture
Low & high risk macro environments
Micro external & internal security zones
Monocultural communication
Location/time-boundedness & centralization as vulnerabilities
Physical protective objects & subjects
Monocultural values, behavior & language
Asset distribution as a countermeasure
Argot & other languages as countermeasures

Figure 7.2: This oversight visualizes the structure of Chapter 7 via a selection of key concepts about the temporal-spatial qualities of deviant security. For a full oversight of descriptive and explanatory key concepts of Part III and their inter-relation, see Figure 9.4.

7.1 Countermeasures Against Data Volatility & Retention

Cyber criminals have an ambiguous relation with volatility and retention of information capital. On the one hand, data volatility and retention work as countermeasures against threat agents, as the respectively irrevocability and availability of information capital for an infinite time might be beneficial to criminals. On the other hand, data volatility and retention create vulnerabilities that have to be patched by business recovery and continuity plans, using a single entity a single time and for a single purpose, or either encrypting or secure-deleting information capital.

Volatility as a countermeasure Because of changed time-space barriers, information assets have become volatile. The problem of volatile evidence from the viewpoint of private and public investigators is well-addressed in the academic literature [502][503][504], and frequently observed in this study. Besides (secure) deletion that is also discussed in this section, cyber criminals try to prevent the disappearance of disappearance by promoting volatility. They will not use, turn off or add functionalities on systems and software to avoid the creation of unwanted data. Because cyber criminals may accidentally infect themselves via their own malware landing page, some disable certain browser functionalities. Others store browser history and cookies, and even run malware [260][440, p.3], on random-access memory (RAM) of respectively their own and their victims' machines. Similarly, the restore system of an operating system is turned off to avoid automated backups; antivirus software on a victim's machine is disabled; virtual keyboards are installed to avoid the risk of keyloggers; virtual machines are used that run on USB sticks; hibernation is turned off; and digital kill switches are added to botnet systems [505].

So, *volatility* works as a deviant countermeasure especially if cyber criminals have stopped committing crime after, for example, big hit *projects* with a longer time-to-task as compared to ongoing business *processes* that have *recency* and *consistency* as vulnerabilities. The latter campaigns have a shorter time-to-task because they continuously generate new data like malware-as-a-service. Investigating historic breaches of big hit projects - like on the US retailer Target [506] - is difficult as the volatility of forensic traces works for the benefit of the criminal. However, stolen information has to be sold and transactions will eventually be detected with all the attendant risks as a result. Yet volatility may also hold blowback effects to the criminal, and this occurred in the following case that a policer officer explained during an informal interview. A member of an access controlled CSAM community lost his collection of abusive images. He had to upload new pictures in order to stay a member, which he desperately wanted. But where to find new CSAM? He was now forced to download images in more open online environments that were unknown to him, but well-monitored by LEA. He was identified and arrested as a result. So, volatility is an example of a benefit related to the commission of crime that may well lead to specific costs in the protection of crime. Volatility further shows that deviant technical computer security is a double-edged sword with *iatrogenic effects*: a term derived from medicine for practices and/or situations that are countermeasure (i.e., medical surgery) and vulnerability (i.e., the complication arising because of medical surgery) in one.

Do not forget your password A money launderer did not write down his very strong password for his Bitcoin wallet as he was worried that LEA might find it during a house raid. He learned the random combination of numbers, symbols and letters by heart and as such it became human capital. Unfortunately, he forgot his password, and as a result he was at the verge of loosing many Bitcoins of his customers which would definitely be seen as an exit scam. He felt his life could even be in danger. Luckily, he remembered that his password was equal to an expired password of a cyber criminal forum account. He explained everything to the administrator of the forum, and begged the admin to recover the expired forum password. The admin explained that he was unable to do so. As a DevSec policy, members' passwords were encrypted when they were in use, and deleted after they were expired. The volatility of intangible assets that the money launderer considered a countermeasure, became a vulnerability.

Business continuity & disruption recovery against volatility Because anything can happen at any time and place, cyber criminals have *business continuity and disruption recovery plans* to ensure the availability of their most important assets. Police raids and search warrants reveal that because of the possibility that information capital is erased due to interrupted memory's power, CSAM users have to rely on nonvolatile storage, like servers, computer's hard drive, USB drives and CD-ROMs to save their carefully collected series. Having multiple C&Cs against botnet takedowns basically underlines the same idea: they are backups. In another observed instance, an autonomous group requested from a BPH previously used IP addresses for their C&C so that infected bots could easily reconnect. Business continuity and disruption recovery may also take other shapes such as the previously mentioned prevention-against-prosecution service that comes to the rescue of suspects of cyber crime. A last example are duplicate identities - also known as doppelgängers - on fora. Generally, having additional accounts on the same forum is prohibited by admins. Indeed, this deception tactic is primarily used to falsely enhance the trust of the main account on a platform by personally vouching for or writing positive reviews about the main account. Additionally, duplicates support business continuity and disaster recovery. When his/her main account is banned because of e.g., violation of terms and conditions, a member still has his/her duplicate account [170]. Similarly, having multiple accounts on various market places ensures that business continues when one forum is taken down.

The cyber-crime-as-a-service economy has responded to the need for business continuity and disruption recovery. Many vital processes in the commission and protection of crime do not have to be self-managed, but can be outsourced to various providers [259, p.7]. Takedowns of botnets are ineffective as long as new bots can be bought at pay-per-install services [399, p.13]. As a result, disrupted processes can easily be fixed or replaced by third-party suppliers. However, the availability of data that business continuity and disruption recovery generates, especially through nonvolatile storages, has serious downsides for cyber criminals as the next paragraph explains.

Data retention in a reversed electronic panopticon Opposite to volatility and going dark is the *disappearance of disappearance* and *going bright.* The first refers to the ability of IT to create and retain informational data within the intertwined networks [507], i.e., *data retention.* The latter is about the increased visibility of cyber criminals and their crimes and related ability of the cyber security to detect and monitor them [147][356]. As shown throughout this study, cyber criminals need information capital to make informed decisions about necessary countermeasures against threat agents. But data retention also works as a vulnerability to cyber criminals. In order to serve a large criminal population, CaaS providers apply *automation* to be scalable, and have client management and support systems and (financial) databases. Criminal assets are not only stored by criminals, but also by other key players, in open and closed sources, in places that the criminal cannot avoid, delete or is even aware of, either saved mentally, physically, locally or in the cloud, and for an infinite time. Malware stored on a version control repository, an account at an online payments system, contact details in domain and IP registrations, a free web based mailbox, but also historical criminal records of suspects who are recidivating: the list of observed vulnerabilities is endless. So, although academics and legal practitioners may report about 'anonymity of cyber criminals', true anonymity is largely a myth in the Information Age. In many instances, there is at most pseudonymity and/or perceived anonymity (see [194, p.107][328]). So from a cyber criminals' perspective, they surely live in an electronic panopticon [50, p.57], which is *not*, as suggested by [28][34][80, p.80], a situation in which few central bodies - most notably governments - have an *information monopoly* on, and are monitoring and investigating, many suspects of cyber crime. For cyber criminals, the electronic panopticon is *reversed* compared to the classic idea of sociologist David Lyon [386].

The reversed version is a decentralized, distributed, fragmented and transboundary panopticon in which important pieces of information about the cyber criminal and his/her crimes are distributed among all key players of the intertwined network. These key players thus go beyond the 'capitalist enterprise' and a 'multitude of state-run institutions' [386, p.666], and includes - but is not limited to - not-for-profit public-benefit corporations ICANN and RIPE NCC, the non-profit digital library Internet Archive and numerous open government initiatives such as commercial registers and tax administrations (see Figure 7.3). After Paunch - the moniker of the creator behind the Blackhole exploit kit, and on any informal most-wanted list of Western cyber crime units for years - was apprehended by Russian authorities and his true name became known to the press, investigative journalist Brian Krebs easily found many 'bread crumbs' on open Internet sources that linked Paunch's online identity to his offline identity including his whereabouts prior to the arrest [366].

This case and comparable stories that are compiled by gathering bits and pieces of incriminating evidence via a range of sources show that cyber criminals not only assign value to intangible assets and physical objects, but also subsequently have to *classify* assets to indicate the required level of confidentiality, integrity and availability. Evidence that links an online moniker to a true identity has to be kept confidential by cyber criminals, while IP addresses of spam servers will be marked as *public unclassified* by the cyber security community after they have been used. Cyber criminals may also classify data incorrectly. In many instances, data is apparently labeled as public unclassified by the criminal, instead of *sensitive but unclassified.* If sensitive data are disclosed, individual snippets of information - timestamps, language configuration, country code top-level domain (ccTLD) - may not cause serious damage. However, the sum of these individual pieces help LEA to build or complete the investigative picture, and may therefore cause grave damage to the well-being of the cyber criminal and/or his/her business.

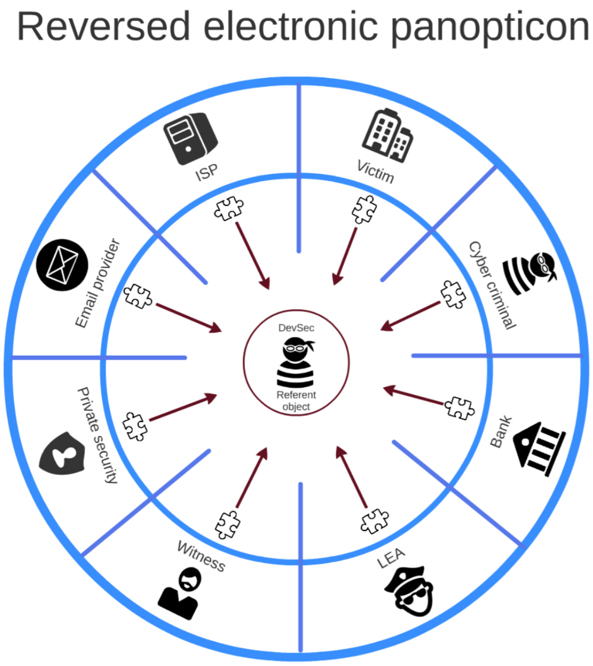


Figure 7.3: In the reversed electronic panopticon, the DevSec referent object is in a *watched tower* (instead of the watch tower). Multiple key players - the watchmen - might hold important pieces of incriminating evidence about the referent object without him/her being able to tell who holds what information.

A single entity, a single time & for a single purpose Because of intertwined networks and the disappearance of disappearance, links are created between various assets related to the criminal and his/her crimes when, for example, multiple integrated Internet-related services and products of a single technology company are used. Cyber criminals try to avoid such connections - i.e., *unlinkability,* an attribute of confidentiality - by promoting *association deniability* and/or *association hiding* (see [36, pp.442-446]). One way to achieve this is a deviant security policy which is based on using tangible assets and/or information capital as a *single entity*, for a *single purpose* and/or a *single time*. Paying a prepaid telephone with cash money and changing its IMEI help to avoid tracks to a true identity, thus enhance its existence as a single, isolated entity instead of an entity that is linked to a subscriber, home address and bank account. The degree of DevSec is increased if the cell phone is only used for a single purpose, i.e., solely criminal usage or to call a particular co-conspirer as compared to contact a range of bonafide and malafide entities with the same telephone. To top it all, a stand alone entity that serves a specific goal should be used only once, such as preventing reuse of cryptocurrency wallets and/or addresses for transactions. Therefore, cyber criminals have been using throwaway email accounts which meet these concerns to a certain extent [508], especially if messages in draft folders are used to communicate with a co-conspirer instead of sending emails to each other. Nevertheless, individuals have to access the mailbox, and therefore leave a (meta)data trail. Moreover, some cyber criminal fora even prohibit registration with a disposable one-time-usage email address as compared to a valid one for structural usage [368, p.6]. The MoneyTaker group applied this security policy - a single entity, a single time, for a single purpose - as much as possible. For each round of attacks, the group deployed a new infrastructure. The attack servers were thus one-time components, specifically configured to deliver a malicious payload to a predetermined list of IP addresses of a single particular victim [440, p.4].

The downside of this policy is that groups generate many more entities that, if not classified correctly and e.g., secure deleted, increase the chance of detectability and linkability by the cyber security community. Using single entities, a single time, for a single purpose, also place a heavy burden on the efficiency of the commission of crime, while traces - e.g., messages - still have to be secure-deleted or encrypted. As described earlier in this section, many threat actors opt for business *processes*, like ongoing malware campaigns. For reasons of efficiency, they may use multiple identifiers, multiple times, for multiple purposes including the same MO [509], additionally generating many live forensic traces which are relatively easily detected and investigated by threat actors which resulted in the discovery of hard links between, for instance, the Angler exploit kit and Bedep botnet [510]. Hypothetically, malafide profit-driven *projects* - a single big hit operation, having the discipline to use a single entity, a single time, for a single purpose - do not have the disadvantage of continuous live evidence about the criminal and his/her crime. As explained before, investigating historic breaches is notoriously difficult as the volatility of forensic traces works for the benefit of the criminal. However, such truly one-off projects seldom occur in practice as incriminating data are generally also created during the post-activity phase of profit-driven cyber crimes (see Figure 6.2). For example, stolen assets of such projects have to be sold on the underground market, creating a path of evidence that will eventually be detected by threat actors with all the attendant risks as a result. Of all investigative cases observed in this study, only the short-lived ransomware outbreaks of (Not)Petya and WannaCry did not lead to any significant post-crime activities. In fact, because the financial schemes behind these crimes were badly drafted to non-existent, experts claim that these two ransomwares might actually have been state-driven attacks disguised as profit-driven attacks by cyber criminals [417].

Secure-deletion of information capital In situations in which cyber criminals cannot prevent the disappearance of disappearance or promote volatility, they will (secure) delete assets to limit the availability of assets, or encrypt valuables for confidentiality. In other words, data has to be wiped so that it is irrecoverable to both the referent object and threat agents, either encoded in such a way that only authorized referent objects can read it, but any threat agents cannot [130, p.5]. Observed manual deletion practices include wiping C&C servers before they are reconfigured by ISPs, deleting posts on social networks, or erasing subscriber information because of data retention laws. Cyber criminals also frequently apply automated deletion as part of their MO, especially when malware distrusts an infected system, see Section 6.6. Rombertik malware overwrote the master boot record (MBR) of the distrusted system and/or destroyed all files in the user's home folder by encrypting each file with a randomly generated encryption key [336]. The Cobalt/Buhtrap malware deleted all its traces with a free and legitimate wiper tool and also removed the MBR [496]. However, because of the information asymmetry about third parties, suspects have little knowledge when threat actors like LEA arrive at the crime scene and what their capabilities are to retrieve deleted data [141][511, pp.39-41]. Figuring out where all data is stored, including copies across systems, may simply prove to be impossible. Even if all the relevant data on a system are found, many users - including cyber criminals - delete data by simply unlinking the file in the file system, while the file remains stored on the system. Dutch court cases against CSAM users show that some users are unaware of the additional steps to truly remove data from the system [512][513][514]. And even if they intend to sanitize their storage media, it is hard to verify that all data traces are indeed made irrecoverable [511, pp.38-39][515][516][517]. This is notably harder if information capital that relates to a criminal identity and business is not under the suspect's control. For instance, a cyber criminal suspect was arrested, and therefore asked a DevSec-as-a-service provider to delete all his support tickets. The vendor did not answer, nor did he delete the tickets with incriminating evidence. Thus both secure-deletion (also known as artefact wiping, and data erasure and clearing [125, p.2]) and, as explained in the next paragraph, encryption are difficult to achieve for cyber criminals.

Encryption of information capital Essentially, encryption is about securing confidential data against a specific threat agent for a *specific period of time*. In other words, after cyber criminals have classified their data, they have to assess the attack capabilities of the threat agents, decide for how long they want to keep their informational capital confidential, and subsequently choose a matching encryption standard. Research shows that intelligence services of nation states would have the resources to build a machine that cracks the most common strength of Diffie-Hellman, and thus decrypt the connections of large numbers of VPNs, HTTP websites and SSH servers [458]. If this is true, cyber criminals - like BPHs - who engage or are misused in terrorist or state-sponsored activities should transition to elliptic curve cryptography, which does not have this weakness. But understanding and applying cryptography is hard for cyber criminals [356, p.15]. In many instances, they are forced to be autarkic as a collective and autonomous as an individual, and thus implement encryption themselves. Yet correct implementation of encryption frequently goes wrong because they lack the knowledge to do so, including the computer-focused criminals behind the Neutrino exploit kit, various ransomwares and the Zeus banking trojan [518][155]. In several Dutch court cases it becomes apparent that some CSAM users also failed to apply encryption correctly, or at least insufficiently against the capabilities of law-enforcement agencies. Encrypted abusive material was sent over an unencrypted but wiretapped line [519], while in other cases material was also found on an encrypted virtual machine [520], and in an encrypted partition and hidden volume [521]. To avoid such problems, encrypted-communications-as-a-service have come to the rescue of cyber criminals, like bulletproof connectivity, hosting and telecom providers. But outsourcing (related to the vulnerabilities of dependency and centralization, see respectively Sections 6.4 and 7.3, and [356, p.15]) of such vital DevSec services may come at a cost. In 2016, the Dutch NHTCU took over several business enterprise servers (BES) that were used exclusively for criminal purposes. The 19.000 users of the network used smart phones which only allowed them to send and receive encrypted messages from other users in the network. Besides their dependency, they must have felt very safe as many of them bluntly spoke about their crimes in the text messages and did not secure-delete this incriminating evidence. In other instances during this study, servers that were discovered deep inside a cyber criminal infrastructure did not have SSL encrypted connections, and could be lawfully intercepted. In those cases, secure-deletion is no longer an option for cyber criminals.

7.2 Intercultural Communication as a Countermeasure

Intercultural communication (IC) as an academic discipline within computer science studies promotes intercultural collaboration of bonafide entities such as communication on computer science research between developers from different cultures or in multi-lingual contexts, see e.g., [522]. There are, however, very few papers about how cyber criminals collaborate and communicate interculturally. Just like bonafide entities [363, pp.9-11], cyber criminals have the opportunity to work online with co-conspirers from very different cultural backgrounds. Computer scientist Ross Anderson argues that it is not technical computer security protocols that tie one computer to another, but:

> ‘ultimately, at the deepest level, this is about anthropology. It’s how systems get embedded in culture, in the interplay of verbal and non-verbal communications’ [523].

Cyber criminals manage to do business with co-conspirers from very different cultures. How do they succeed? The answer lies within intercultural communication: an academic discipline that evolves around the central question how people understand one another when they do not share a common cultural experience [524, p.1]. The next paragraphs first explain the building blocks for intercultural communication in cyber crime, before moving on to weaknesses in

IC and introducing the concept of intercultural communication as a countermeasure.

Intercultural communication in cyber crime: context Three building blocks are of importance in IC: context, communication and culture [363, pp.52-53]. While the emphasis in this section is on the latter two building blocks, *context* is crucial to understand the economical, historical, physical, political, social and technical situations and structures in which (intercultural) communication between cyber criminals occurs [363, pp.52-53].

Because of the Great Firewall of China that probes and blocks circumvention proxies, almost all Chinese CaaS fora are physically hosted in China; only a single Chinese forum was discovered as a Tor onion site during this study. Compared to Russian and English-speaking cyber criminals who opt for Jabber chat protocol with OTR to interact online, their Chinese counterparts prefer Chinese commercial chat services like QQ and WeChat [367][420]. In these instances, we have to understand the political context of China on a macro level, and its effects on technology usage in meso and micro environments.

Furthermore, there might well be differences in intercultural communication between e.g., vendors and clients on fora, as compared to IC between cyber criminal organized groups that do not sell any services on online markets. Indeed, criminal organizations from different cultures also collaborate, but (so far) in complete darkness to academics. Yet the Russian-language Carbanak group, as a review of the related investigation reveals, used Chinese exploits and had other (undisclosed) links with China as well in 2014. Such Sino-Russian cyber criminal links were not observed so far. In this particular case, we have to consider social contexts between cyber criminal individuals on a micro level.

Because the focus of this study is on intercultural communication on fora, we further have to acknowledge that there might also be considerable differences between communication platforms as they have, for instance, their own history. Cyber criminal forum Darkode resurrected as a Tor onion site after its takedown by the FBI in which many members were arrested as well. The Russian-language forum Verified was hacked, and its backend was subsequently leaked on the Internet [525]. It might well be that the deviant security culture on the fora changed after such events. In both instances, we have to acknowledge the historical context of cyber criminals collectives on a meso level. In short, context matters when we study intercultural communication of cyber criminals.

Intercultural communication in cyber crime: culture The above mentioned Darkode, dubbed the most prolific English-speaking hacking forum by Europol [526], was taken down by the FBI in 2015. Although the forum had over 300 active users, over 70 arrests were made in at least 20 countries around the world. So, English was a lingua franca for cyber criminals who came from non-English dominant contexts. Similarly, Russian is the common language *(lingua franca)* for citizens of the Commonwealth of Independent States, large parts of Central and Eastern Europe and Northern and Central Asia - Русский мир ('Russkiy mir') - but also on cyber criminal forum Verified [525]. Likewise, there are also - amongst others - Brazilian, Chinese, German and Japanese cybercriminal communities, and each community has their own (preferred) communication platforms, such as CaaS fora on the open Internet, cryptomarkets or legitimate social media [527][421][420]. Yet surprising cross-cultural collaborations between communities can be found, such as computer-focused Brazilians who search for help in the Russian CaaS underground [528], but also Dutch drug traffickers who recruit computer-focused criminals to hack the computer systems of a sea port terminal in Belgium [529], and traditional organized criminals who work - as several investigators confirmed - with computer-assisted criminals to launch phishing campaigns. But culture is much more than the nationality of these suspects: they have different occupations, relation status, living conditions and education, and belong to different socioeconomic classes, religions and sexual orientations to name a few. They therefore probably also have different world views, behaviors, norms, values and beliefs, feelings and emotions [363, p.32]. This is all known as *subjective culture*, and very much the focus of most intercultural communication scholars [524, pp.2-3][530, p.211]. Culture is software of the mind, and everybody, including referent objects of deviant security, are programmed by culture [531].

Darkode and Verified as exclusive, unilingual/bilingual fora are not a standalone cases. Fora are *not* homogenous, global and universal market places, but differ in offered products/services, members, size, and very much in culture. Cyber criminal fora have their own distinctive cultural features that go beyond language. Private security researchers of antivirus vendor Trend Micro describes how fora not only differ in accessibility and offered products/services, but even atmosphere. For example, Russian fora have a 'very standoffish feel to it', according to the researchers, as members do not reveal any personal identifiers in their postings [532]. Cyber criminals may express the values, norms and beliefs of their larger dominant legitimate culture on a macro level, that way shaping the micro subculture of the cyber criminal forum. For example, a review of relevant terms and conditions shows that CSAM is strictly forbidden on English and Russian-language cyber criminal fora, and most BPHs from these undergrounds claim to apply a zero-tolerance policy against the abusive material. So indeed, *taboo tradeoffs* do exist within the underground. These vendors have sacred values protected from material gains (similar to cyber criminals who will not attack citizens of their home country, although they face *tragic tradeoffs* when profits are so high that they reevaluate their principles). Yet CSAM is allowed on Japanese CaaS fora [533], reflecting the relatively tolerant attitudes towards sexual depictions of children in Japanese society [534]. Disdain for the law in general [535][536][537], and approval of certain hacker values - like unlicensed software usage - are widely accepted in Russian and Ukrainian society [538, pp.114-115], even by state institutions and large enterprises [479]. In this sense, the legitimate dominant culture may overlap with the criminal subculture. Thus, not only the commission of cyber crime is much more embedded in local culture than many academics expect [539][364], but the protection of crime and the criminal as well.

Cyber criminal undergrounds differ in deviant security
The Russian-language CaaS underground can be characterized as an ecosystem with a closed community that deploys many administrative controls that are separated from one another such as trust, distrust and distribution mechanisms (e.g., multiple well-enforced bureaucratic rules and referral mechanisms). The English-language cryptomarkets, on the contrary, are open communities that have technically integrated security mechanisms (think of the mandatory usage of Tor, and integrated escrow services, encrypted communications and payment systems based on crypto currencies, see Figure 7.4). Chinese-language cyber criminal fora, however, miss out on many *ex-ante* and *ex-post* controls to prevent, detect, deter and correct insider and outsider threat agents. Chinese fora lack many of the above mentioned administrative and integrated technical security mechanisms. Integrated technical countermeasures - Tor, cryptocurrencies - are difficult to implement in the heavily regulated/restricted and monitored Chinese cyberspace. Apparently, the same goes for many administrative countermeasures. Let us take the *ex-post* control of moderating as an example to explain this issue. The observed Chinese fora and chat groups are poorly moderated. This is not surprising with platforms that have so many members generating so many posts and messages. Members frequently spam other members, while many of them send off-topic messages. Furthermore, Chinese forums usually do not label vendors based on trust as English and Russian-language do, i.e., VIP, verified seller, unverified seller, guest and/or ripper. Instead, forum members expose rippers in public threads, usually with their unique chat number, their forum alias and/or the modus operandi of the ripper. Cyber criminals not only use this method of openly shaming rippers on illegitimate fora, but on legitimate Chinese (commercial) communication platforms as well.

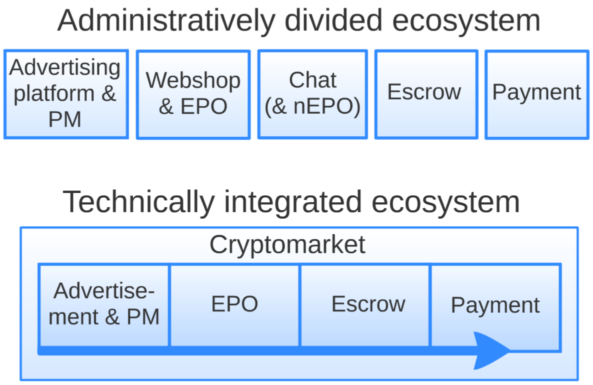

Administratively divided ecosystem
Advertising platform & PM
Webshop & EPO
Chat (& nEPO)
Escrow
Payment
Technically integrated ecosystem
Cryptomarket
Advertise-ment & PM
EPO
Escrow
Payment

Figure 7.4: In the Russian-language CaaS ecosystem (depicted above), various channels - from a forum with advertisements and private message system (PM) till payment services - are generally separated, optional and non-consecutive. This means that customers visit an advertised web shop and fill in an electronic purchase order (EPO), or close the deal directly via a separate chat channel and thus place a non-electronic purchase order (nEPO). Moreover, transaction partners can negotiate payment systems and the need of an escrow. Like a few Russian-language 'all-in-one outsourced online shops' [540], English-language cryptomarkets are technically integrated ecosystems with consecutive steps of mandatory EPO, escrow and payment (depicted below).

Intercultural communication in cyber crime: communication *Communication* is an expression of culture [541]. Generally, communication consists of language: nonverbal behavior/body language, speech/spoken language and writing/verbal codes [530, p.454]. According to interviewed private security researchers, cyber criminals do use audio and video conferencing technologies to conduct interviews with potential co-conspirers, although voices might be masked, video turned off and traffic ported through an anonymity service like Tor. However, the emphasis in this section is predominantly on writings like public posts and private messages via fora, chat and email.

The importance of written texts to cyber criminals is apparent throughout this study as communications may reveal much about the criminal and his/her crimes. Several previously mentioned deviant countermeasures (e.g., deception, trust mechanisms) and legitimate attacks (e.g., authorship analysis) are mostly based on written texts by a single individual (e.g., malware code) or between persons (e.g., business transactions through chat or fora). Strikingly, when criminals are communicating online through chat or fora, they have nothing more than writings to develop complex relationships. High-context cultures - like China, Great Britain and Japan - place much emphasis on nonverbal actions (e.g., haptics, kinesics and proxemics) and paralanguage (speech behavior like intonation, pitch and volume) to communicate [542][363, pp.173-188][530, pp.454-455, 531][524, pp.10-12]. Yet online intercultural communication between cyber criminals on fora largely occurs through writing and not through face-to-face contact. This may have considerable benefits for the commission of crime as online communication filters out much of the prejudices related to physical attributes on which we base our first impressions such as age, clothing, tattoos or race [363, pp.280-282]. At the same time, intercultural communication, and more specifically (sub)cultural language use, also affects deviant security practices: it works both as a weakness and countermeasure against threat agents.

Vulnerabilities of intercultural communication via conversations There are serious vulnerabilities in intercultural communication that may pose a threat to the assets of referent objects. The first weakness is due to conversations with other persons, including co-conspirers and threat agents. Of course, authorship analysis exploits the vulnerability that written texts and even system configurations are attributable to individuals. Chat conversations of a known cyber criminal might be used to identify his/her unknown moniker on fora. However, authorship analysis cannot always be applied, nor is constantly needed in police investigations. Still, there are other weaknesses in communications between cyber criminals that will help law-enforcement. Consider that there are different fora for each stage in the career of a cyber criminal. Young and aspiring, but unskilled offenders - script kiddies - are not allowed on professional CaaS fora as they do not have the right referrals or offer any unique products or services. Their criminal career starts by discussing minor crimes on online game and piracy fora, and will then move on to more dedicated script kiddie fora [543, pp.474-477]. These fora may be in their own language (e.g., Dutch), or in a familiar second language (English) as explained in the text box below. Nevertheless, both their nonverbal behavior and writings are very specific and local as compared to abstract and global. In other words, it is easy to identify an individual in the early stages of his/her criminal career, because he/she still misses human capital on DevSec, and conducts behavior which is related to the legitimate dominant culture and less to the criminal subculture. They are more likely to tell others in which country and/or city they live, which sports team they support and which crimes they commit(ted). They are also more likely to make specific linguistic errors in second language usage that will reveal their native tongue (called *interlanguage* [363, p.163]). Writings in a common language of a forum like English allows identification of the native language of non-native English authors. This method is known as *native language identification* [544]. These examples further show that *code switching* - changing communication styles between dominant and subcultures [363, p.153] - is still difficult for aspiring cyber criminals with little human capital about DevSec. The problem that criminals face is that native language identification is hard to avoid, while changing language patterns might erode trust between business partners.

Fora serve cyber criminal careers
Script kiddies start their criminal career by discussing minor crimes - e.g., defacements and DDoS - on relatively harmless fora (read: low threat fora), like gaming platforms. Although there are major English and Russian-speaking low threat fora, there are also relatively many platforms in other national languages. These script kiddies are potential key enablers of cyber crime. Some stay thrill-seeking adolescent-limited offenders, but others become more persistent, financially-driven offenders and move on to medium threat fora. The latter platforms evolve predominantly around the commission and protection of cyber crime. Some nationalities are now forced to opt for a forum with a different language as their linguistic group is just too small to cater them. For example, no professional Dutch language cyber criminal fora were observed during this study. These tomorrow's key enablers are in the transition to grow from amateur to professional cyber criminals. The impact of their profit-driven crimes and the degree of security are still relatively low but increase as their human, organization and information capital grows in time. Their services and products are largely unknown to the cyber criminal and cyber security community: they are in the process of building a reputation among and relations with co-conspirers, and searching for niches in the underground economy. They will have a presence on dedicated carding fora/shops and fora with few well-known services/products (read: medium threat fora), and/or have a low member status on more professional CaaS fora (read: high threat fora). Today's key enablers are financially-driven, and form the top tier of the cyber criminal underground. As compared to the other two groups, they have the best and most (access to) tangible and intangible assets. Their reputation, services and products are well-known to the cyber criminal and cyber security community. They are very much brands, and are high in the commission and protection of crime. They only work with other professional conspirers, or are able to serve large groups of less professional cyber criminals as they automated their business model. They solely advertise their services/products on exclusive English or Russian-language high threat CaaS fora, and have a high status on these fora. Some of these professionals will stop advertising their products/services on fora as they want to limit their visibility and already have a fixed group of professional clients. Still, they might have a presence on medium and high threat fora to buy services and acquire knowledge.

Vulnerabilities of intercultural communication via software and systems Individuals may also communicate through software and systems, and indirectly and probably mostly unintentionally deliver a message to threat agents as well (although intentional threat messages in ransomware code directed at a specific AV vendor have been observed). Consider again malware code and the associated threat of authorship analysis. The written code directly communicates with a computing system, but indirectly communicates with mandated breachers and security researchers whom try to retrieve the code and apply reverse engineering and/or authorship analysis. Written texts - whether data or software - are an inherent weakness of MOs, and reveal much about the criminal's gender, age, ethnicity, occupation, intelligence, skills, and, ultimately, offline identity. Although research that goes beyond attribution of writings is nonexistent, several security researchers in this study stated that malware can be very 'Chinese' or 'Russian', based on the structure of the code and their general look and feel. As witnessed in this study, a malware sample contained the word 'shokolad' in Latin spelling that was probably translated phonetically from the Russian word in Cyrillic spelling шоколад (meaning chocolate in English). Similarly, the instructions to business partners of the Ponmocup botnet were written in Cyrillic [391, p.6]. Such clues are very important to start and/or narrow down a criminal investigation (see also [19, p.19]), and/or make informed decisions which private or public partners should be involved. Using Dutch language in malware code as happened in Coinvault and TorRAT [545][397], attracted unwanted attention of Dutch LEA, and resulted in arrest of the suspects. Registration practices and IP behavior are other examples of weaknesses in intercultural communications. Script kiddie fora have less a deviant security culture as compared to more professional platforms. Hence, their members are still relying on the online practices of their dominant culture, and are therefore more prone to use their real IP and email addresses when subscribing to a forum. Because of the poor DevSec culture on the forum, they indirectly communicate identifying information to potential threat agents. In an observed instance, a Dutch script kiddie used his real IP address until he gained the knowledge to hide his IP address. After he successfully tested a VPN, he proclaimed online to others that the PET worked, but then continued to use his home IP address again. Such cases prove that code switching is not only necessary in written software code, but also in nonverbal behavior as third party threat agents may extract important information out of criminal conduct.

A battle of nonverbal security behavior: VPN usage on fora
The identification and block of duplicates - members with two accounts - is a task of administrators on fora. Admins may log all IP addresses and receive a notification when two different accounts use the same IP address to access the forum. They may launch an investigation, comparing registration and posting practices and time stamps. However, this deviant security mechanism becomes useless when members use the same VPN connection to securely access the forum because they have the same bulletproof connectivity provider. The inbox of the admin will then be flooded with false positive notifications. This example shows that referent objects not only have different security interests, but also that related countermeasures may compete against one another, rendering one of the two useless.

Third culture & deviant security culture It is argued that intercultural dialogue between law-abiding entities is difficult to achieve in online environments because of - amongst others - anonymity [546, pp.225-226]. However, professional cyber criminal fora like Darkode and Verified are examples of successful online subcultures because of that very same anonymity. Indeed, even if members understand each other linguistically, they still have different cultural backgrounds and (thus) communications styles. Therefore, they try to adapt to each other, and end up constructing a new communication style, i.e., a *third culture* [363, pp.153-154][546, pp.223-226]. So, criminal subcultures may have overlap with a legitimate dominant culture, but can also completely be distinguished from it [547, p.46]. Related to the former, investigative journalist Brian Krebs discovered that the Russian-language CaaS forum Verified used 'cultural captchas'. Visitors had to answer a question that related to the Russian legitimate dominant culture in order to enter the forum [548]. Likewise, Japanese cyber criminal platforms use captchas that requires visitors to enter only e.g., Hiragana or Kanji characters [533, pp.8-9]. DevSec culture *is* communication and emerges, like any other culture (Hall in [549, p.777]), through interaction. Because members face similar deviant security problems, the issue of protection is an extremely important issue to its members to the extent that cyber criminal third cultures can be characterized as *deviant security cultures*. In other words, these third cultures provide a climate with unique security-related values and norms in which individuals can safely interact with each other. A forum should be an online home, i.e., a place of safety and security which is especially true for CSAM fora where members are relatively free to express their sexuality. Culture in general, including deviant security culture, is learned behavior [363, p.32], thus involves human-, information-, and organization capital. If members do not value security, they will not adopt security policies, nor buy DevSec products and services. DevSec culture is achieved by promoting *intercultural communicative deviant security*: the understanding of cyber criminals that communication between individuals or groups of different cultural origins has inherent vulnerabilities but simultaneously works as a countermeasure against threat agents. Again, identity plays a key role to understand DevSec, not only as a vital part of the definition for this study's definition on modus operandi, but also in intercultural communicative deviant security. Cyber criminals, similar to law-abiding entities [363, p.94], express or hide their identities to or from others through communications. Their online identities that evolve around DevSec in order to be successful, are negotiated, co-created, reinforced and challenged through communication with key players. Ultimately, deviant security will become part of the newly created cyber criminal identity of - amongst others - forum members which occurs through monocultural communication.

Monocultural communication as a countermeasure Although profit-driven fora may have many members from very different dominant cultures, some of these online market places exist over ten years. These fora - including platforms for sexually-driven CSAM [550] - are therefore clearly *long-time* *persistent* as compared to *adolescence-limited* fora that never reach a sufficient maturity level. Member activity on the latter fora stops because they do not promote the commission of crime enough, e.g., too few members or unique services/products (including content), or because they have too many vulnerabilities, and as a result are taken down by threat agents. An example of such a failed forum for stolen credit card information was the platform Carders.de. This forum was unable to distinguish rippers from 'bonafide' carding vendors [454]. Indeed, successful fora apply necessary technical countermeasures against a range of threat agents and related attacks. Yet another reason that these places are successful safe havens is because of a softer control: their members excel in intercultural communicative deviant security.

So how should we characterize this intercultural communicative security on successful fora? The answer is that the writings and nonverbal behavior on these fora are largely homogenous and abstract. In other words, these newly created third cultures prescribe *monocultural communication* to promote the protection of business and identity (see Figure 7.5). The nonverbal behavior and writings of individuals are so homogenous and reveal so little about their identities that they work as a security mechanism against law-enforcement. So, *convergence* (see [530, p.456]) on monocultural fora occurs when members try to minimize cultural differences by matching communication practices of other members. As a result, *intercultural conflict* by internal threat agents is avoided, while outsiders like mandated breachers are having a hard time to say something about the cultural background of individuals, even if large amounts of written texts (e.g., forum postings and chats) and metadata (timestamps, IPs, email addresses) are available. Let alone that outsiders are able to blend in: cyber security researchers are frequently detected and subsequently expelled from cyber criminal collectives like carding fora and shops [551][552].

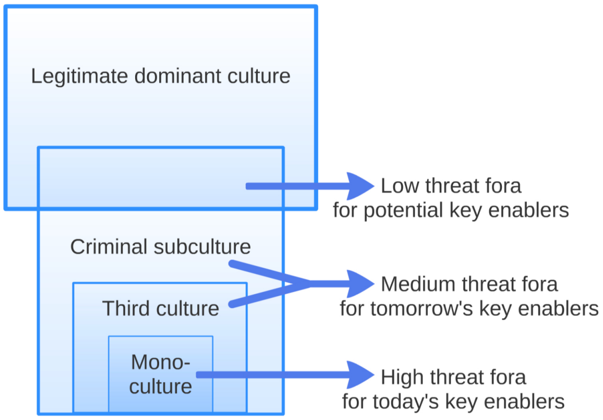


Figure 7.5: A dominant culture influences a criminal subculture. A third culture, however, is a newly constructed subculture with its own communication styles and could manifest itself as a cyber criminal monoculture.

Monocultural values, behavior and language Monocultural communication is similarity-based, and prescribes common i) values, ii) behavior and iii) language [524, p.1]. The most striking example of prescribed monocultural *values* in third cultures is that members are united around a single goal and have similar deviant security interests. Topic threads generally do not undermine the main aim of a profit-driven or sexually-driven forum, respectively selling cyber criminal products/services and sharing CSAM. So, members do not express their political or religious views, as such avoid *value conflicts* (see [363, p.233]). Terms and conditions of fora generally prescribe to their members not to insult and/or offend others by means of hate speech, derogatory remarks and so on.

Prescribed monocultural *behavior* are mandatory usage of prescribed DevSec mechanisms on e.g., cryptomarkets: Tor to access the platform, electronic purchase orders, mandatory escrow, member status and an integrated payment system, see Figure 7.4. Through such *rule-based and role-based controls* that provide *accountability* [454, pp.39-40], deviant security practices are simplified for individual members, DevSec managers (like admins) and the larger community. These controls provide a *paternalism* solution as they enhance and influence individual choices to increase the members' security as a private and club good [553, p.74].

Lastly, monocultures may further require that its members use just a single *language*, therefore enhancing its monocultural climate, see Figure 7.5. So, some cyber criminal fora only allow the Russian-language which works as a countermeasure against any threat agent who do not speak Russian (see also [453, p.4]). Members who are not fluent in Russian are admonished [320, p.11], while observations show how those who had used other languages or automated translations were expelled from the fora. This security policy might be influenced by the Russian dominant culture in which thinking in terms of 'we are surrounded by enemies', 'us and them' and 'ours and strangers' is not uncommon (indeed, Russian exploit kit vendor Paunch knew English and sold his product on Darkode [366]. This might be explained by the hypothesis that he is a Western-oriented Russian citizen) [530, pp.90-94]. In reaction to this strict single language policy, a number of cyber criminals have their advertisements translated manually into Russian by translators then post them on the forum. So, national languages can work as a countermeasure, and the next paragraph dives deeper into this subject.

Argot and other languages as countermeasures Third cultures, including monocultures, may further promote the use of *argot*: the language of the underworld that supports the idea of intercultural communication as a countermeasure against threat agents [554]. Albeit following the grammar rules of the dominant culture, argot is the vocabulary of the third culture as it is artificial and nobody's mother tongue [547, p.47]. Argot is learning another language (*language acquisition* [363, p.161]), and as such becomes human capital. Cyber criminal argot, like other argots [555], supports the commission of crime by promoting - amongst others - an online identity, inner group solidarity and an alternative social structure [543][547, pp.52-53, 56]. However, argot also works as a countermeasure against threat agents, and can be further explained by technical computer security concepts like the CIA triad:

- *Availability*: argot provides the technical language to insiders to discuss the specifications and nuances of deviant security. In the Russian-language underground, BPHs and their clients speak about дедики (‘dedyky’) and абузоустойчивый хостинг (‘abuzoustoychivyy khosting’) when they are talking about respectively dedicated servers and bulletproof hosting, while money launderers and their clients use the words лошадь (‘loshad’, literally meaning horse in English) and дроп (‘drop’) to refer to respectively money mules and offline/online locations where fraudulent transfers are sent to.
- *Integrity*: argot helps to exclude threat agents from a closed subculture. Incorrect usage of argot, as well as a sudden change of communication style, will raise suspicion among cyber criminals. The former situation points to outsider threat agents like noobs and undercover agents who do not have the vocabulary (i.e., human capital) to communicate with professional cyber criminals. The latter situation may point to insider threat agents, like co-conspirers who turned into criminal informants, and their sudden change in communication style has been observed several times during this study.

‘How ya doin, mate?’
A forum member was discussed by other members when one of them noticed that his language usage was very different than usual during a chat conversation. Was his account compromised and taken over by a threat agent? The member in question was later approached by some of the members via another communication platform and he explained what happened. He stated that he had not logged out his chat session in an Internet cafe, and that somebody else must have replied to incoming messages with his chat account.

- *Confidentiality*: argot further thwarts investigations by concealing knowledge about malicious activities. Writings are very important to prove criminal intent about cyber crimes. The legal difference between bulletproof hosters and bad hosts is that there is evidence that the former knows what his/her criminal client is doing on his/her server, and therefore is a co-conspirer for the crimes that his/her client commits [459, p.21]. Even if there is correspondence between criminal hoster and client, argot may conceal/obscure conversations about crime, and thus intent.

Besides argot, rare national, minority and/or regional languages may work as a countermeasure against threat agents as well. For LEA specifically, language works as a delaying mechanism that increases the double whammy effect of DevSec, hampering any police investigation as it absorbs scarce resources (i.e., capacity, access to linguists, budget and time). Generally, American and European law-enforcement agencies have information positions on cyber criminal communication platforms where the common language is either a European (including

English) or East Slavic language. Yet there are virtually no investigators in these agencies that have the combined tactical, technical *and* cultural/language skills to grasp the full extent, true nature and various aspects of cyber attacks. For instance, Dutch police investigators encountered an organized money mule group in the north of the Netherlands whom spoke the local Frisian language mixed with argot. All intercepted telecommunications had to be translated to Dutch, while the interpreters in turn had difficulties with the carder argot and technical jargon. In such a situation, both automated and manual translations may express the meaning of the words, but not the sense of the conversation. This problem of identifying the meaning of words in context is also known as *word-sense disambiguation* [556], and very relevant to those who are confronted by deviant security. The focus, related investments and subsequent methods of working of Western LEA - i.e., separation of digital, linguistic and tactical investigative roles - to understand especially the Russian-language underground economies have another downside, namely: undiscovered crime caused by other language groups. According to a reviewed intelligence report, an individual of Moroccan descent who lived in Europe sold his malware on predominantly Arabic-language cyber criminal fora. He would probably not have been detected if he had not revealed personal details on an English-language forum.

7.3 Distribution as a Countermeasure

Cyber criminals, infrastructure and victims are easily distributed across locations on various levels of aggregation with protective qualities against threat agents. Indeed, mutual legal assistance treaties between states aim at overcoming distribution as a countermeasure by harmonizing national procedural and substantive laws. As mentioned before, states might intentionally and unintentionally provide deviant security. The next paragraphs dive deeper into this issue and other issues, and show countries, including but not limited to their laws and policies, play an important role in the protection of crime and the criminal. This section subsequently discusses the impact of a geopolitically multipolar world on deviant security and how countries can be distinguished in various points of attack and low-risk and high-risk areas. Cyber criminal MOs with little understanding of these dimensions are vulnerable when too much centralization, while sticking to the same location for a considerable time, is applied. Therefore, referent objects may distribute their assets as a countermeasure. Ultimately, these temporal-spatial qualities add to the distributed, decentralized and fragmented nature of a reversed electronic panopticon.

The multipolar world as a countermeasure Cyber criminals may well be geographically stuck in jurisdictions that they cannot or do not want to leave for private or professional reasons. On the one hand, they are increasingly a ball in a game of power politics played by various political blocks, both for the better and worse. The world is becoming increasingly post-Atlantic and *multipolar* [557]. This fundamental shift in the global pecking order will have geopolitical repercussions and consequences for the international legal order [558]. The previously dominant legal doctrines and approaches of the US and EU have been replaced by significant national and regional differences in Internet governance [559]. These different views on Internet governance lead to legal pluralism on security, privacy and executive power [560]. Similarly, IT is not necessarily a 'liberation technology' that promotes fundamental rights and freedoms [561]. On the contrary, information technology has helped multiple authoritarian regimes to strengthen control over their citizens, leading to arrests of political dissidents that were labelled as 'suspects of cyber crime' [39]. Moreover, governments accuse and counter-accuse private security firms of alleged ties with intelligence agencies of other countries and subsequently restrict these companies from operating in their jurisdictions [562][563], adding to the creation of cyber security networks along geopolitical lines. Whether this multipolarity and diverse usage of IT by governments will lead to more competition or cooperation on cyber crime issues remains the question. It is, however, apparent that major political blocks are opting for an Internet that is much more centralized in its governance [564], because - amongst others - cybercriminals are empowered by the generativity of the Internet [565][163, p.107]. Although it is unclear what cyber crime laws of which block will be the dominant rule worldwide, it is further apparent that cyber crime laws, policy and investigations will increasingly become an expression of, subjected to, and shaped by, geopolitical situations and international relations. In other words, cyber crimes have become means of exerting pressure on, and leverage between, states. As long as domestic cyber criminals do not harm or even promote national interests, governments may have political incentives to deliberately ignore, encourage, coordinate, order or even integrate attacks by criminal citizens on overseas jurisdictions, by providing e.g., support, operational details and immunity [566][360][567][568]. As a result of such government actions, suspects escape *accountability.* This practice further shows how deviant security continuously changes through time and place because of - amongst others - dynamic macro level geopolitical situations. Ultimately, the distinction between deviant, public and state security is becoming increasingly blurred. Instances have been observed in which there was substantial evidence that financially-driven cyber criminals were conducting state-permitted, state-sponsored and even state-forced attacks, while simultaneously receiving necessary protection of their government against the law-enforcement agencies of the countries under target.

On the other hand, cyber criminals adjust their security to specific events, settings and situations that occur on a macro level. Reasons why many Russian-language cyber criminal platforms are hosted outside the Russian Federation might well be tightening Russian Internet regulations [569], and/or the evasive Russian lawful intercept and surveillance program SORM (Система Оперативно-Розыскных Мероприятий - 'Sistema Operativno-Rozysknykh Meropriyatiy') [570]. Cyber criminals actively exploit legal and policy loopholes in jurisdictions, international conflicts and geopolitical blocs as many other examples show in the next paragraphs. However, such 'smartness' may turn against them, precisely because national laws on cyber crime still widely differ and jurisdictions set different priorities for various offenses [262]. For instance, an observed individual only delivered technical support to a cyber criminal organization knowing that such acts were not punishable under his national law, i.e., *nullum crimen sine lege.* Yet under law of another jurisdiction, he was considered a co-conspirator - i.e., a suspect of crime - that knowingly provided vital services to cyber criminals that attacked victims, and received stolen money as a payment.

Points of attack origin, linkage and occurrence To understand how a geopolitically multipolar world and the disappearance of time and space barriers further help cyber criminals in commission and protection, we first need to recognize that cyber crime consists of three interrelated components that give LEA jurisdiction to start an investigation. Simplified: i) cyber criminals need ii) infrastructure to make iii) victims (see also [571]). Each of these three components may be located in different places which make cyber crimes indeed truly transnational. Legal scholar Susan Brenner calls the location from which cyber criminals operate *points of attack origin* [17, pp.409-424]. She further names the areas where (potential) victims are based *points of attack occurrence* [17, pp.425-429]. Unmentioned in the literature are those locations where financial, legal and technical infrastructure of the cyber criminal are located. Cyber criminals have to connect to the victim's network via botnet C&Cs, process stolen money, and register offshore shell companies to protect their assets. As Figure 7.6 depicts, these financial, legal and technical networks are best dubbed *points of attack linkage*, as they connect the referent object to others like cyber criminals and victims. From a legal perspective, these connection points are just as important as the other two points of attack because state authorities will have jurisdiction to start an investigation when e.g., a single bank account, legal person or malicious server is in their territory. The geographical location of cyber criminals, infrastructure and victims, and the political, economical, and cultural situation in those areas, have a major impact on the security practices of cyber criminals. These three points of attack can be placed on a continuum that ranges from low to high-risk areas. The former locations contribute to the security of cyber criminals, while the latter hold serious security-related exposures to cyber criminals.

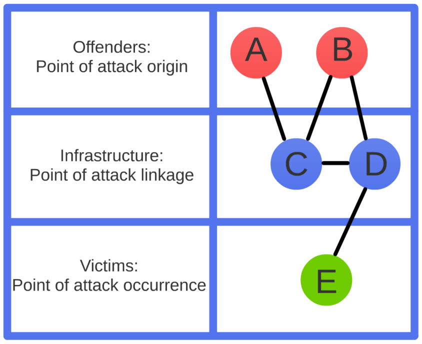


Figure 7.6: The introduction of points of attack linkage helps to understand how referent objects, (financial, legal and technical) infrastructure and victims are inter-related. Offenders who are located in jurisdictions A and B may use infrastructure hosted in jurisdiction C to communicate with each other via chat, email and/or fora. They may further use infrastructure in jurisdiction D - such as a C&C server - to attack victims in jurisdiction E.

Low-risk macro environments The physical locations that pose the lowest risks for cyber crime are *safe havens*. Reasons why areas become safe havens are the existence of cyber criminal communities that are well-developed in both nature and extent. Not only are there large numbers of active cyber criminals based in such an area, but their members also have (access to) high quality and large quantities of tangible and intangible assets such as investment capital, highly skilled co-conspirers and optimized criminal business processes. Generally, the cyber criminal communities in *low-risk areas* have the upper hand as the cyber security community experiences opposite circumstances. Besides deliberately abetting to deviant security, key players from the cyber security community in these jurisdictions may also be cooperative in confronting cyber crime but are inadequate, and thus unable, to do so [566, pp.2-3]. Safe havens lack an active, well-developed cyber security community, and are plagued with a large double whammy effect. These locations have no effective cyber crime laws, policies and/or enforcement because of corruption, few adequate resources and little cross-sector collaboration [364]. Generally, safe havens are associated with point of attack origin [572][573][283][54][574][575][538]. However, points of attack occurrence and linkage can also be safe havens as shown in Figure 7.7. Distributors of child sexual abusive material regularly shift their material between jurisdictions that are considered weak on enforcement [20, p.394]. Servers in countries that have internal conflicts have been used by cyber criminals as enforcement against misuse will be low. So, C&Cs of the botnet GameOver Zeus have been hosted in Eastern Ukraine since 2014, while BPHs have been offering servers in Syria since the year 2012. Servers in the latter country lend themselves for confidentiality as few countries could successfully send an MLAT for a preservation request to the Syrian government. Yet botnet herders, phishers and spammers may choose *availability over confidentiality*, and may therefore, besides techniques such as double fast flux [576, p.1], prefer countries without an effective Internet governance policy to reduce the amount of malicious traffic, like the Netherlands [577][578][579]. Besides low costs and high-uptime of Dutch servers (needed for the bots to contact the C&C server), botnet traffic to and from the Netherlands will be a less detectable anomaly for intrusion and detection systems of Western European banks and ISPs than traffic to and from, say, Iran. Equally, established ISPs in relatively well-governed jurisdictions control the bulk of botnets, and Dutch ISPs might have incentives to hold a passive attitude towards botnets such as the cost of mitigation and pressure of regulatory involvement [162].

Just like traditional criminals [283, p.173], cyber criminals attack *preferential markets* where benefits are high and costs are low, like malware that are sold as pay-per-install and exclusively target the UK and US [399]. Points of attack occurrence might simultaneously be a preferential market and a low-risk area. CSAM offenders target vulnerable children in economically disadvantaged countries. Financially-driven criminals successfully hacked financial institutions in less IT-advanced countries like Bangladesh, Gabon, Iraq and Vietnam, and transferred large sums of money via SWIFT [580]. Both areas hold high benefits (e.g., children, money) and low security risks because of an ineffective cyber security community.

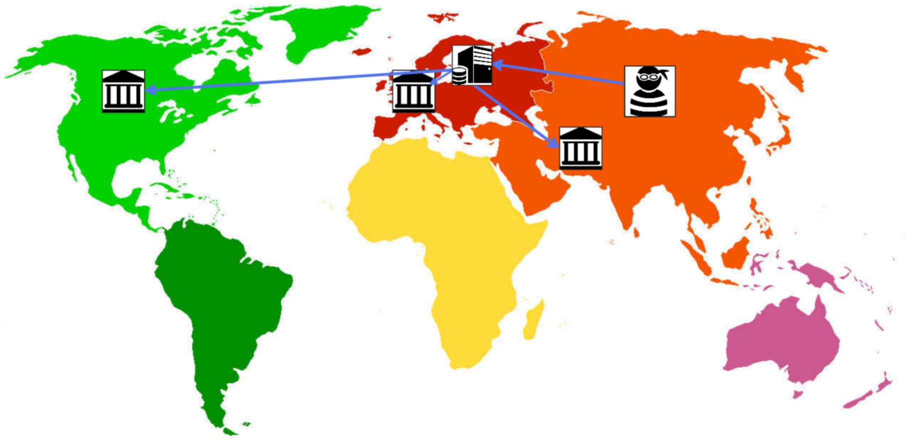


Figure 7.7: This visualization is an example why some jurisdictions can be regarded as low-risk areas. From e.g., a Dutch LEA perspective, cyber criminals who are located in jurisdictions (read: points of attack origin) with whom the Netherlands has no effective legal treaties operate from low-risk areas. They may misuse Dutch technical, legal or financial infrastructure (read: point of attack linkage) - e.g., servers, legal persons or bank accounts - to make victims in other jurisdictions, including the Netherlands, the US or their own country (read: points of attack occurrence).

High-risk macro environments On the other side of the spectrum are jurisdictions that are labelled as *high-risk areas.* These countries have installed effective cyber crime laws and policies, and dedicated cyber crime public institutions that serve the public interest. The larger cyber security community proactively shares intelligence and collaborates against threats and attacks. A multistakeholder Internet governance model is installed, and prevents, detects and takes down malicious server activities. Potential victims keep their security up-to-date, while actual victims are willing to inform appropriate public agencies by filing a complaint. The hypothesis is that suspects of cyber crime who operate from high-risk areas must take more precautions against the cyber security community than cyber criminals who are located in low-risk areas. Referent objects that are based in high-risk areas are less developed compared to the cyber security community in their jurisdiction. They possess fewer assets and do not get the opportunity to mature into a well-developed cyber criminal community as explained later in this paragraph.

Whether an area becomes a high or low-risk is not solely determined by the quality and quantity of bonafide threat actors of cyber criminals. Macroeconomic factors may have an impact as well, such as the technical educational level of the working population [538, p.114], and gross domestic product (GDP), Internet users per capita and unemployment rates [581][582]. This position is also backed by a game theory experiment that indicates that crime in economies with plenty of well-paid IT jobs only pays for average hackers: ‘very good professionals who have high probability of getting maximum payoffs from legitimate activities are not prone to engage in criminal activities’ [583, p.53]. Less talented hackers will have little DevSec-related human and organization capital, and as a result, are more vulnerable to successful legitimate attacks from well-resourced LEA. For instance, the Netherlands has a well-developed cyber security community [270], unique language, and a chronic shortage of qualified information technology workers [584][585]. With some notable exceptions like the autonomous TorRAT group and very specialized CaaS providers like bulletproof hosters, one could therefore consider the Netherlands as a relatively high-risk point of attack origin with generally mediocre home-grown computer-focused criminals. This position is not only backed by empirical findings of this study, but also by research of other scholars. Leukfeldt, Kleemans and Stol reviewed eighteen Dutch police investigations on phishing networks from the Netherlands. They concluded that the majority of networks only targeted the Netherlands with low-tech attacks. Only two high-tech and two low-tech cases had some international links with victims and offenders operating from multiple countries [179]. To conclude, there is not only a *digital divide* between cyber security communities from low-risk areas and high-risk areas [56], but also a divide between cyber criminal communities in low-risk and high-risk areas, see Table 7.2. The next paragraph takes a look at how location and time-boundedness and centralization negatively affect the security of the cyber criminal’s micro environment.

Digital divides between communities	*Cyber criminal community in low-risk areas (CRI-LR)*	*Cyber security community in low-risk areas (SEC-LR)*
Cyber criminal community in high-risk areas (CRI-HR)	CRI-LR avoids direct interaction with CRI-HR as a co-equal transaction party. CRI-HR might become clients of CRI-LR for automated bulk CaaS, such as selling stolen credit card credentials or email addresses, or when collaboration is absolutely necessary like the provision of moneymules (known as drops).	No instances have been found in which CRI-HR targets points of attack occurrence that are both preferential markets and SEC-LR. Yet this observation might be caused by a dark figure of undiscovered cyber crime. SEC-LR in point of attack occurrence will not have the means to investigate these attacks, while SEC-HR in point of attack origin rather focuses on attacks that target their own jurisdiction (i.e., point of attack occurrence).
Cyber security community in high-risk areas (SEC-HR)	SEC-HR focuses on CRI-LR when the latter regards the former's location as a preferential market (i.e., point of attack occurrence). However, SEC-HR can only successfully arrest and prosecute when CRI-LR travels to SEC-HR [358].	SEC-HR faces a collaboration paradox with SEC-LR. One the one hand they need SEC-LR for execution of their legitimate offensive countermeasures against CRI-LR such as arrests and takedowns. On the other hand, SEC-HR risks damage to these countermeasures because of the large double whammy effect in SEC-LR, including corruption.

Table 7.2: This matrix describes the digital divides and collaborations between cyber criminal and cyber security communities in high and low-risk areas.

Location and time-boundedness & centralization as vulnerabilities Cyber criminals may use malicious servers, or bank accounts where stolen money is deposited, for too long. If criminal practices are conducted on the same location for a considerable time, they become noticeable to the outside world. As a result, these spaces may become high-risk areas, thus increasing the chance that legitimate interventions against the malicious activities are launched. This happens when the three points of attack are continuously located in the same jurisdiction, including larger jurisdictions such as of the sum of states that ratified the Cyber Crime Convention, or within the same geopolitical bloc. Although the administrators behind a large DDoS booter and main technical infrastructure were located in different jurisdictions, all points of attack origin - Canada, Croatia and Serbia and United Kingdom - and points of attack linkage - Germany and the Netherlands - ratified the Cyber Crime Convention, with arrests and takedowns as a result [272][586]. Many simple cyber crime investigations -

considered low-hanging fruit by law-enforcement officers - start because cyber criminals, used Internet infrastructure and victims are in the same jurisdiction for a considerable amount of time, like the multiple DDoS attacks that were launched by Dutch script kiddies on one of the largest access providers in the Netherlands [587]. So, cyber criminal assets are *bounded by temporal-spatial dimensions* which work as a vulnerability. This is also apparent in the fixed 9AM-5PM working hour patterns of criminal hackers that subsequently reveal the time zone in which they are located [588], after workday peak hours of CSAM downloaders [589], or the tradeoff of Bitcoin tumblers between mixing chunks with many mixes for a short escrow period each or few mixes with a longer escrow period [403, p.497].

The problem of location and time-boundedness does not end here. MOs with too much *centralization*, while sticking to the same location(s) without interruption, make things even worse for cyber criminals. Centralization of assets leads to a *single point of vulnerability (*or *single point of failure*, [156, p.121]), and has been observed at different aggregation levels. More specifically on the level of countries, legitimate security and DevSec providers (respectively bonafide email providers [356, p.13], and the previously mentioned criminal BES with 19.000 users), IP-ranges and individual servers, and even software and data on these servers like cyber criminal fora. According to Moura's research on online bad neighborhoods [213], twenty ISPs were responsible for half of the spamming, while one Nigerian ISP was found having 62% of its IP addresses involved with spam. Phishing and spam were mostly located in respectively the United States and Southern Asia. During this study on DevSec, many instances were encountered in which cyber criminals centralized too many functionalities on a single server. In a successful attack on several financial institutions, a dedicated server was simultaneously a connection to the victims' systems, storage room for attacker tools and stolen data, a Tor hidden server, and a place from which a hack on a shared web hosting server was launched. Lastly, dominant cryptomarkets such as Alphabay, Hansa and Silk Road, and cyber criminal fora like Dark Market and Darkode are also examples of locations with too much centralization. They were places where too many high value targets of LEA met (for a similar problem with Bitcoin mixers, see [456][590]). For today's key enablers of cyber crime, there is actually little choice in suitable high threat fora with enough equally skilled peers whom offer quality products/services. This *lock-in* relates to both legitimate and illegitimate products/services, and is a major vulnerability for the cyber criminal underground. Cyber criminals subsequently face a tradeoff between on the one hand access to and availability of other cyber criminals and a range of products/services, and on the other side their own individual security, e.g., confidentiality of identity.

Asset distribution as a countermeasure Cyber criminals, and even complete underground economies as previously shown in Figure 7.4, may avoid centralization and location-boundedness and time-boundedness. They make compartments of assets, and separate information, (malicious) software, systems and individuals and their duties and roles within organizations. Cyber criminals may use several servers in attacks, and separate their functionalities. One server is used as a C&C, a second and third server function as backup C&Cs, another server is used as storage, while a fourth server is used to host a carder shop. Similarly, organized groups may have strict job positions, thus apply role-based functions, such as crypters, hackers, money mule managers, malware developers and web designers. If a group member stops due to resignation or arrest, he/she is easily replaced which protects business operations.

We now link assets (*what*), compartmentation and rule-based and role-based controls (*who*) to the when and where. The subsequent *distribution* of these compartments in intertwined networks not only provides availability but may also increase confidentiality. More specifically, distribution limits the visibility of assets to threat agents because of the attribute of *unlinkability*, and as such the *anonymity* of the criminal and the *unobservability* of crimes (see [207]). More specifically, criminals will extent the evidence trail, and replace, scatter and/or rotate assets in a decentralized manner. In other words, distribution is a countermeasure and can be executed through *extension, replacement, rotation and dispersion* (see Figure 7.8).

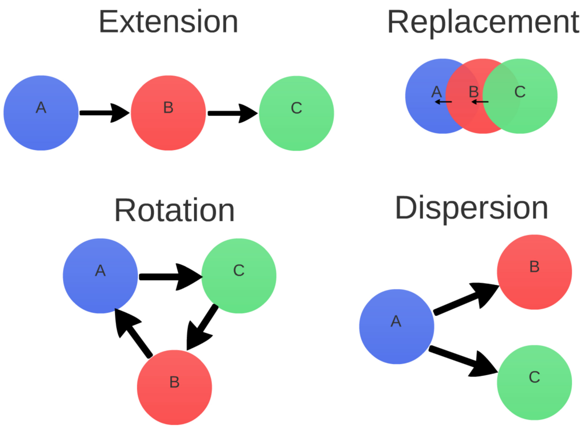


Figure 7.8: Distribution as a countermeasure consists of four techniques: extension, replacement, rotation and dispersion.

The following examples of transnationally operating botnets further explain distribution as a countermeasure:

- *Extension*: Super peers of p2p botnets work as proxies that extend the chain to the valuable botnet panel. Cyber criminal sites like fora and DDoS booters may use anti-DDoS services, re-directing authorized traffic through an additional server, and filtering out any attacking bots [591]. However, these services also work as an extra link - a proxy - in the chain which obscures the true IP address of the forum, and delays any interventions taken by LEA.

- *Dispersion*: Many of the observed botnets in this study usually have number between three to five C&C servers at any given time. These points of attack linkage are often scattered among multiple jurisdictions and ISPs to exploit low-risk areas in today's multipolar world.
- *Rotation*: Botnet C&Cs may rotate between ISPs in different jurisdictions after a certain period of time or particular event, like a newly infected, high-value victim. This tactic prevents LEA in the affected country to respond adequately [592, p.586].
- *Replacement*: Botnet C&Cs may use DNS fast flux to protect a fully qualified domain name by having an enormous amount of IP addresses assigned to it which are frequently swapped [593]. Furthermore, malware developers frequently repack, thus replace, their wares up to twice daily to evade detection by antivirus software [399].

Be aware that extension, replacement, rotation and dispersion might be jointly executed, on various levels of aggregation, in an automated fashion, and not only by botnets like Ponmocup [391, p.30], but in other cyber criminal schemes as well. To avoid attribution, cryptocurrency tumblers (see e.g., [403][328][330]) not only work as an extension, but essentially separate incoming transactions, replace them with other transactions, and scatter the outgoing transactions among the users of the service. Distribution as a countermeasure can also be mixed with other controls, providing additional proof for how deviant security is very much applied in compensating layers. The example about online dead drops for CSAM in Section 3.2 is generally a combination of i) distribution as a countermeasure (i.e., extension via a third party file sharing service), ii) usage of a single entity, a single time, for a single purpose (a hyperlink to the service for each individual CSAM download), and iii) automated deletion after the material is downloaded.

Still, extension, replacement, rotation and dispersion are difficult to accomplish. Besides additional implementation costs, these policies only work if cyber criminals avoid repetition and apply a degree of *randomness*. Repetitive patterns in MOs not only provide linkability to attacks on victims, but also generate a new weakness - i.e., *predictability* - which is frequently exploited by defenders and mandated breachers. Ultimately, cyber criminals face an unavoidable tradeoff between *deviation versus conformity*. Outliers in e.g., time patterns - a lot of activity on Sunday morning, instead of standard weekly working hours - will raise the interest of the cyber security community, while that same consistent working pattern is exploited by LEA to make informed decisions when a suspect is at home to make an arrest and/or search his/her house.

Fight, flee and/or serve your country
How do successful cyber criminals deal with high-risk areas in macro environments? They have to adapt to the situation (an intangible asset), and either fight or flee. *To fight* in this sense means staying in the high-risk territory, and trying to turn their micro environment into a low-risk area (see Section 7.4). The Dutch cyber criminal group TorRAT that targeted victims in the Netherlands were presumably forced to apply this strategy, and implemented a security-driven approach. Their MO was extensively built - amongst other things - around being highly autarkic, including developing their own malware and laundering the stolen money themselves, and applying countermeasures against data retention and volatility (deletion, prepaid cards, privacy enhancing technologies), deception (installing Zeus malware on infected machines as disinformation) and distrust (usage of preconfigured dongles) [348]. Another option is to target victims in-, misuse Internet infrastructure of-, and/or allocate other assets in low-risk macro environments, including the cyber criminal's own physical presence (*flee*). There are a number of relevant stories from interviewed participants about such distributions of cyber criminals, infrastructure and victims. Several Russian cyber criminals who targeted Russian businesses fled to Ukraine because Moscow was not in contact with Kiev after the civil unrest that started in Eastern-Ukraine in 2014. In another instance, an American cyber criminal went to Moscow, and subsequently targeted the US. He was later arrested by Russian authorities as requested by American LEA. The Moscow-based group that used the malware Dyre tried not to attack Russia and the US. The group probably expected that were operating in a low-risk area as they avoided making Russian victims: according to several participants of this study, Russian legal proceedings require *de facto* an identified victim to open an investigation in Russia while suspects subsequently have to be caught in the act of заливы ('zalivy' - the act of stealing money from a victim's bank account as compared to merely delivering e.g., technical support to such a financially-driven computer-focused MO). Nevertheless, group members were arrested by Russian authorities in 2016. These examples underline that the sequence of cyber criminals from the CIS who attack the preferred markets of the United States and Western Europe, does not necessarily apply. Still, there are many examples in which East Slavic-speaking cyber criminals did intentionally avoid attacking the Russian Federation and/or the larger Russian-speaking world (see also e.g., [418, p.83]). The CryptoWall ransomware did not infect computers with Cyrillic configurations, and Russian-speaking victims could request a decryption key for free. This corrective countermeasure was presumably applied to prevent Russian LEA from acting against CryptoWall. Similar to the banking trojan Dridex [594], the Wildfire ransomware code excluded IPs of infected machines from the larger Russian world such as Belarus, the Russian Federation and Ukraine. Lastly, profit-driven cyber criminals stated to potential business partners that they would never attack their motherland, while sociocultural norms of the dominant legitimate culture may dictate that stealing from the West is not necessarily a bad thing [538, p.114].

7.4 Physical Deviant Security

So far, this study has addressed mainly administrative and technical controls of cyber criminals against threats from cyberspace. The physical, offline world is important to referent objects as well, not only for commission [215, pp.41-42, 68], but also because of protection. From a good guy perspective, physical controls protect assets like facilities, personnel and other resources [59, p.28]. Yet this section shows that deviant security of a physical nature may differ from prescribed industry standards. This section starts with the vulnerability of asset conversion from the online, intangible world to the offline, tangible world. In the physical realm, cyber criminal referent objects opt for limited territorial control and operate from micro external and internal security zones. This section then focuses on physical DevSec on the most micro level: physical protective objects and subjects, more specifically access control, surveillance, and violence. Lastly, the vulnerabilities of deviant physical security standards are discussed while Table 7.3 summarizes the observed physical controls of this study. A methodological remark is that many of the collected data sources of this section are derived from a single point of attack origin, more specifically the Netherlands, which is considered a high-risk area for cyber criminals. Data about cyber criminals located in other countries are used to a lesser extent. It is expected that this difference between points of attack origin - being either a high-risk or low-risk area - has an effect on the nature and degree of physical security controls.

Online & offline asset conversion As described in Section 5.4, both tangible and intangible assets are an inherent component of cyber crime. How to interpret the relation between the tangible and the intangible from a deviant security perspective, more specifically the cyber criminal's online and offline world? Events in the cyber criminal's online micro environment are threats to his/her assets in his/her offline micro environment, and vice versa. In many cases, digital forensic research on a server may discover a home IP connection that points to a physical location. Subsequent house searches, preservation of hardware and possible arrests may generate, in turn, evidence and intelligence about (other) crimes in the online world. There is such an interplay between the online and offline world, that the distinction between what is digital and what is physical has become *blurred*. This is especially visible in online sexual violence against children [85, pp.46-48, 114]. A victim of CSAM may disclose the exploitation at some point in time, while the images can provide lasting evidence that sexual abuse indeed has taken place. Similarly, besides data carriers like USB sticks, passwords written down on pieces of paper and printed out information security manuals were also found during house raids.

The psychological and technical merge of these two worlds [595][596][192, pp.66-67], may wriggle for cyber criminals because of - amongst others - the previously mentioned removal of time-space barriers. While they are physically bounded by time and location, their online activities are not. In an operation against Blackshades - a malicious trojan horse that controlled computers remotely - law-enforcement found new investigative leads after a house search of a Blackshades administrator located in one time zone, and quickly preserved data in other time zones. An associated Blackshades administrator, who was still asleep because he was located in a different time zone when the preservations were executed, could only respond hours later when much of the damage to his infrastructure had already occurred. Notably, many non-IT focused objects are in the transition to become IT focused objects. Nowadays, automobiles are rather hardware and software on wheels, and help legal practitioners by generating - amongst others - incriminating information capital (read: evidence) about the cyber criminal and his/her crimes [597].

Computer-enabled criminals buy physical assets on cryptomarkets that will be send by legitimate postal delivery services to a physical location and this practice promotes detection by LEA (see also [598]). Computer-focused and assisted criminals face a similar but slightly different problem: the conversion from intangible to tangible valuables, and vice versa. In other words, transfers from the online world to the offline world and the other way around. Indeed, the previous example about child abusive material points to this issue of *asset conversion*. CSAM are depictions of physical sexual abuse, and as such, conversions from the tangible to the intangible. The audio, images and videos frequently contain important clues about the who, where and when of the physical world. Based on child sexual abusive images, the Dutch police reconstructed the room in which the abuse took place, and successfully showed the three dimensional model to the general public: the mother of the child victim recognized the room of her house and called the police. Likewise, several cyber criminals have been observed who posted clips on social media in which they showed events that occurred in their private life. More than once, such uploads revealed to investigators - amongst other - the suspect's place of residence, car ownership and/or associates. The vulnerability of asset conversion also works from online to offline. Profit-driven cyber criminals may prefer to cash their stolen virtual money in hard currency. In several instances, money mules had to visit corrupt bank employees, or ATMs to withdraw money which made them visible, thus vulnerable. The Lurk group launched a campaign in Russia to re-issue SIM cards of ordinary citizens in order to commit online banking fraud. However, sending and collecting the physical SIM cards made them vulnerable for detection by a variety of threat agents from the cyber security community [260].

‘We had a drink together the other night’
It is striking how little information there is in academic studies about the direct physical surroundings of cyber criminals. Most research about cyber criminals and their crimes evolves around their digital world, such as used forums, malware and botnet infrastructure. Yet cyber criminals need physical subjects and objects for the commission of crime as well as the protection of the criminal and his/her crimes, as shown in Section 5.4. Similar to findings by Leukfeldt et al. [196, pp.6-8][195], an observation of this study is that some cyber criminals know their co-conspirers physically. Communications between computer-focused cyber criminals proved they are acquainted in real life as well (hence the title of this box which is derived from two cyber criminals who discussed a third individual: ‘[He] is doing great. I had a drink with him the other night’). Other examples include the group of 80 individuals behind the Dyre malware that worked from an office in the financial district of Moscow [253], and several Dutch CSAM users who met in person to exchange encrypted hard drives with abusive content and/or discussed plans to sexually abuse children. Furthermore, several cyber criminals, especially cross-cutting criminals such as online money launderers and money mules [599, pp.20, 56-57], were detected because of offline crimes, such as shoplifting, physical abuse or illegal possession of firearms. For instance, a woman fled out of a department store because of shoplifting and lost her bag with her passport, birth certificate and some letters with her postal address in the Netherlands. Because of a hit based on that personal identifying information in Dutch police systems, she was linked to an ongoing investigation against the group behind the MYFL malware [600]. Lastly, several occasions were observed in which co-conspirers had to install malware on, or withdraw money from, ATMs and reported to malware developers whom were based in another jurisdiction. These are additional arguments why cyber crime has more local and offline dimensions than one may expect at first glance [539][364]. Cyber criminals live in a physical world, and are as such affected by their direct physical surroundings.

Limited territorial control Physical security is part of many industry standards on technical computer security, and includes crime prevention through environmental design (CPTED) and target hardening of IT facilities [59, pp.435-442]. Researchers have looked at how traditional criminals - especially drug dealers - have applied defensible space principles for law-abiding citizens to protect themselves from their own threat agents creating *offensible spaces*: a safe place to conduct crime [601][602]. What are the characteristics of the cyber criminals’ offensible spaces? Let us start with their *territorial definition* - the physical micro environment that is under control of the cyber criminal, more specifically, point of attack origin. The participants of this specific section about physical security - mostly computer-assisted and computer-focused criminals located in the Netherlands - differ from traditional criminals in reviewed literature (most notably, drug dealers based in the US [317]) in the sense that they do not control public spaces, but merely their direct private surroundings. Dutch cyber criminals live in a high-risk physical area, and must minimize their visibility. Thus, they opt for a limited physical sphere of influence. This is explained by their cyber criminal MOs. Physical environments - especially public spaces - are less important for the commission of cyber crime as it is to - let us say - drug dealers. Physical space is far more important for the protection of the cyber criminal and his/her cyber crimes. In other words, control over large territories does not help cyber criminals in generating more financial profits. Similarly, cyber criminals do not opt for *territorial reinforcement* to emphasize or even extend their sphere of influence so potential threat agents feel unwelcome. On the contrary, reinforcement strategies over large territories rather work as a vulnerability. Thus, cyber criminals have to limit their control to mostly non-IT focused physical objects in which vital IT focused physical objects reside, or in other words, to the buildings in which the necessary hardware is located to commit cyber crime. An undercover agent rang the bell of a suspect's house and played a script. The suspect did not buy the excuse, and talked to the distrusted stranger while using the chain door lock. He closed the door, shut down his computer and even called the police to report the incident. The argument of limited territorial control is further supported by the limited physical control that cyber criminals have over objects and subjects in points of attack linkage and -occurrence. These points do frequently not coexist with point of attack origin, and can thus not be physically governed but rather via administrative and technical countermeasures. For point of attack linkage, bulletproof hosting resellers and their clients rely on ISPs with physical data centers. The bulletproof reseller makes *upfront costs* by renting these servers from the ISP prior to reselling them to their criminal clients. He/she then protects these IT focused physical objects through administrative security mechanisms like moving activities from one server to another and technical security measures such as full disk encryption on a dedicated server. However, the installment of physical countermeasures - e.g., CCTV - to detect whether a law-abiding ISP collaborates with LEA against him/her and/or whether his/her servers are preserved or intercepted is generally not an option (nota bene, fast flux service networks suffer a comparable restriction of no physical subject/object control, see [576, p.5]). Similarly, when points of attack physically converge, such as ATM malware that have to installed physically on the cash machine like Alice, ATMitch, Ploutus and Tyupkin, territorial control is also limited. On the contrary, the physical protection measures of ATMs - alarms, CCTV and guards - may actually harm the criminal and his/her crimes [494].

Micro external & internal security zones How could we further define the physical security policies related to the building form in which Dutch cyber criminals reside and have their operations room in point of attack origin? To answer the question, we first have to divide the building form in a continuum. This continuum ranges from a *micro external environment*, the exterior with more potential threat agents, attacks, vulnerabilities, risks and less control by the cyber criminal, to a *micro internal environment*, the interior with less potential threat agents, attacks, vulnerabilities, risks and more control by the cyber criminal. This raises the next question: which security policies deal with these continuum? House searches show that Dutch cyber criminals divide their physical environment into *security zones* with different protection levels. On the outer sides of the spectrum - the micro external environment - cyber criminals opt for an environmental design that allows them to blend in into their direct physical surroundings as much as possible. Cyber criminals who are based in the Netherlands need to deceive their direct physical surroundings about their true intentions. To prevent becoming an anomaly and to avoid the suspicion of outsiders, they have to hide the real and show the false and merge with the area around them. The premises in which Dutch cyber criminals operate did not differ from the surrounding buildings. No cases have been found in which cyber criminals had installed physical countermeasures that were seeable from the outside such as barb wire, outside CCTV and additional concrete walls while neighboring houses did not have such visible security. These observations support the idea that highly visible security mechanisms in the cyber criminal's micro external environment rather work as a vulnerability as they alarm potential threat agents.

In the inner core of the spectrum - the micro internal environment - referent objects have their operations room and apply target hardening - read: install more visible protective measures - which are discussed in the next paragraph. For young criminal hackers who live with their parents or law-abiding room mates, bed rooms provide the best place as an operations room. This is understandable as parents and room mates may detect the criminal activities and are thus potential breachers. According to investigators, CSAM users who live with their family may create a restricted and controlled 'hobby room' where they can view the material in relative safety. If individuals within the direct social surroundings are not deemed potential breachers, other rooms can be used on the premise as well. A cyber criminal in his mid-twenties lived with his digitally illiterate mother. He conducted his digital crimes from the dining table in the living room. His shocked mother stated to the investigators after his arrest that he frequently showed her on his laptop 'how he earned his money with something called "Bitcoins"' without any further explanation where the cryptocurrency came from.

Physical protective objects and subjects Two physical security mechanisms are most apparent in the micro external and internal security zones: *access control* and *surveillance*. Natural surveillance exploits physical features of the micro environment to observe threat agents. Based on observations, review of investigations and interviews with investigators, both computer-focused and computer-assisted offenders (like suspects of CSAM) who did not live on ground floor, placed their computer purposely near a window that allowed them to overlook the street in front of their apartment for any potential threat agent. Conversely, a CSAM user was caught by window cleaner while he was watching the abusive material. Technical surveillance was discovered during house searches; a rogue spy shop, for example, had deployed hidden cameras. Besides these physical protective objects, cyber criminals can also covertly monitor (potential) threat agents like LEA, co-conspirers and victims. In other words, physical surveillance conducted by physical protective subjects. Similarly, access control can also be divided in natural, physical and technical access control. The former and latter consist of the installment of physical objective objects, the middle is conducted by subjects. Natural access control includes armored doors and hiding objects. Technical access control includes digitally remote-controlled and analogue kill switches. No instances of physical access control were found. This would require a situation in which - amongst others - front desks and security guards (read: protective subjects) would limit the access of unwanted visitors which is imaginable in the Dyre case. The group behind this malware rented an office in the financial district of Moscow, and subsequently pretended to be a legitimate movie company [253]. Because surveillance mostly has preventive and detective goals, it must be followed up by other countermeasures including access control. A reviewed investigation showed how two high-value CSAM suspects lived next to each other in a small village. Both had installed kill switches that could be operated from their own house. Likewise, computer-focused criminals had established a text message system that informed co-conspirers to destroy evidence when ordered. All these physical access control and surveillance mechanisms are very much of a defensive nature.

Yet defensive countermeasures alone might not be sufficient to protect assets. In an operation against the Avalanche botnet, a cyber criminal used an assault rifle to shoot through an armored door at a SWAT unit of the Security Service of Ukraine (SBU). This incident is one of many examples in which physical protective subjects apply the offensive countermeasure of *violence*. Violent acts are of a physical or psychological nature, and are executed for preventive, deterrent and corrective purposes. Violence further points to physical security layers for which there is substantial evidence that this is also a security practice for cyber criminals. Examples are cyber criminals that sent heroin, a funeral cross and a SWAT unit to a security researcher [603][604]. CSAM producers may threaten a victim to prevent that he/she discloses the abuse. A cyber criminal heavily resisted (read: fought back) during his arrest by a SWAT unit. He succeeded in pulling a kill switch connected to his desktop, and as such avoided that LEA could access his turned on computer system. Overt observations by handlers discourages co-conspiring money mules to commit acts that harm the collective. Lastly, violence can be corrective, for example, when a co-conspirer is responsible for an incident. Physical or psychological punishment may rehabilitate him/her and allow him/her to reintegrate into the group. For instance, two clients were unhappy with the attitude of a malware developer and stated that ‘he is the type of guy that needs to be taught a lesson by beating him up’. Similar to deception, violence can be inherent to the commission of crime and have protective side effects. ‘How-to-abuse-children’ manuals on CSAM fora recommend preventive controls such as abusing very young children whom are unable to disclose about what happened and using lubricants to avoid detectable bruises [390].

The vulnerabilities of deviant physical security standards Physical countermeasures of cyber criminals may differ from industry standards. No good guy guidelines or principles on physical security are found that stipulate that individuals must place computer displays in front of a window, use violence against intruders or hide objects. What are the vulnerabilities of *deviant physical security standards*? Firstly, instances were observed in which cyber criminals did not apply any physical security at all which increases the risk that threat agents

Physical controls	Enforced by	Examples	Preventive	Detective	Corrective	Deterrent	Recovery
Access control	Objects	Natural: hiding objects*, fortified doors	X			X	
		Technical: offline and online kill switches, GPS and cell phone jammers					
	Subjects	Physical: front desks, security guards					
Surveillance	Objects	Natural: workplace in front of the window to overlook the street		X			
		Technical: CCTV, recorders					
	Subjects	Physical*: covert (counter) observations					
Violence	Subjects	Physical: assault, overt (counter) observations	X		X	X	
		Psychological: threats, verbal abuse					
		Sexual: rape, sexual abuse					
	Objects	Technical*: DDoS and TDoS	X				
Physical backups*	Objects	External hard drives					X
Corruption*	Subjects	Bribery, impunity	X	X	X	X	
Physical distribution*	Subjects	Relocating operation room	X			X	
Physical deletion*	Objects	Destruction of hardware	X				
Compartmentation*	Subjects	Organizational cells	X				

Table 7.3: The basics of security policies marked with an asterisk (*) are discussed in more detail in other sections and chapters.

are able to harm assets. The absence of physical security is understandable. In some situations, physical security is very hard, if not impossible. Besides the described situations in which points of attack converge like physical ATM hacks, other examples include a construction worker in the Netherlands shared a small bungalow with multiple fellow workers. His room mates watched a movie on his computer while he was gone, and easily discovered his CSAM collection on his computer. Another CSAM user was noticed by a passenger while viewing the material in the train. In other instances, observed physical protective objects were installed, but not of a state-of-art nature. Although available in legitimate spy shops in the Netherlands, no biometric access controls or professional power backup systems were encountered during house searches. Most encountered measures were part of a very limited and improvised toolbox. Not complying to industry standards may further lead to extremely dangerous work places for the referent object. A cyber criminal attached a self-made kill switch to a door. When the door was opened by unauthorized individuals - read: threat agents - the computer would turn off. However, the switch generated electric sparks and could easily cause a fire. Similarly, not obeying direct orders of law-enforcement officers may lead to the risk that legitimate violence is used against the referent object of deviant security, and may constitute a new crime and/or be an aggravating factor in sentencing.

7.5 Interim Conclusion and Discussion

The purpose of this chapter was to describe the temporal-spatial qualities of deviant security. Not only can DevSec practices be explained in microeconomics terms such as information monopolies, (value) conflicts, preferential markets, paternalism, taboo and tragic tradeoffs, and tradeoffs as availability versus confidentiality and deviation versus conformity. Protection of cyber criminals is also understood by concepts derived from linguistics and social sciences - notably anthropology and criminology - such as association and political deniability, code switching and subjective culture.

On countermeasures against data volatility and retention *Data volatility and retention* can both work for and against cyber criminals which shows the iatrogenic nature of DevSec: some practices and/or situations are vulnerability and countermeasure in one. To protect themselves against losing assets, cyber criminals have business continuity and disruption recovery plans installed. At the same time, so many data nuggets about the cyber criminal and his/her crimes are retained by a number of key players in intertwined networks that there is a reversed electronic panopticon. The referent object of DevSec is in a watched tower (as compared to a watch tower) without him/her being able to tell which threat agent holds what information against him/her. Cyber criminals have several policies to deal with both data volatility and retention. Such strategies include using a single entity, a single time, for a single purpose, and secure-deletion and encryption of information capital. Despite evidence that especially autonomous cyber criminal groups apply business continuity and disruption recovery after takedowns of infrastructure by the cyber security community, questions remain what patterns can be found in their plans. For example, on what moment do referent objects have the most upfront costs. Equally, researchers have shown how basic pay-per-install (PPI) providers use plain HTTP, hard coded URLs and unencrypted downloaders, while advanced PPI providers have encrypted C&C protocols and executables [399]. The question remains what the adversarial evolution is for both commission and protection providers on DevSec in general and encryption specifically. In the light of the current going dark debate, a further study could assess what intangible assets are generally encrypted and which not, and if cyber criminals in general, and malware crypters specifically, have certain encryption preferences, and if so, why.

On intercultural communication as a countermeasure Another significant finding to emerge from this study is how cyber criminals communicate interculturally for both commission and protection as cyber criminals do not necessarily share the same linguistic and cultural origins. The research first applied the three general building blocks of *intercultural communication* - context, communication and culture - to the cyber criminal underground. This subsequently allows to understand the vulnerabilities of IC for cyber criminals, whether weaknesses that occur because of writings (thus data) between persons, or through written code in software or non-verbal behavior on systems. This study then explains how intercultural communication works as a countermeasure against threat agents to the extent that successful cyber criminal platforms can be characterized as monocultures. Moreover, the specifics of protective language, e.g., argot which is so important in the underground in general and monocultures specifically, is researched. Language issues in general are an important topic for future research. It is unknown if native language identification is applicable to short messages full of slang and argot. Furthermore, there is also a need to identify the native language of individuals who use automated translation services to communicate with e.g., Russian-language cyber criminals. Other research directions may include applying the organizational and national cultural dimensions theory of psychologist Geert Hofstede on cyber criminal communication platforms, and measuring the power distance, individualism, masculinity, uncertainty avoidance, long term orientation and indulgence of these collectives [531]. Other questions point to the relevance of the cultural, linguistic and social anthropology of deviant security. Why are certain Russian-language cyber criminals using the Latin alphabet to communicate with Russian-language conspirers, and how that is perceived by other cyber criminals?

On distribution as a countermeasure Criminal assets are *distributed* for protective purposes because of macro level geopolitical situations such as an increasingly multipolar world. Basically, there are three important locations that give LEA jurisdiction: i) cyber criminals are located at point of attack origin, and ii) use infrastructure at point of attack linkage, iii) to attack victims whom are located at point of attack occurrence. These points of attack can be placed on a continuum that ranges from low-risk to high-risk areas with respectively weak and strong cyber security communities. A major vulnerability for cyber criminals in these points of attack are MOs with too much centralization, while sticking to the same location(s) without interruption (i.e., location-boundedness and time-boundedness). Therefore, they distribute their assets through four DevSec policies - extension, replacement, rotation and dispersion - which might be jointly executed, on various levels of aggregation, and in an automated fashion. To develop a full picture of distribution as a countermeasure, additional studies will be needed that provide descriptive and, ideally, predictive statistics about how frequently e.g., specific C&C servers are rotated, replaced, extended and/or diffused. What is the abuse cycle of of bulletproof servers, i.e., the purchase, configuration and usage by cyber criminals, subsequent identification and notification by the cyber criminal community, and response by the BPH? What are working day/hour and travel patterns of referent objects, which events create outliers, and why (like interventions by the cyber security community, or bank/national/regional public holidays, e.g., the finding that Dridex banking trojan activities dropped significantly in the week of Orthodox Christmas [605])?

On physical deviant security The last section of this chapter moves from the online world to the offline world of cyber criminals, and addresses their *physical deviant security.* The interplay between the intangible and tangible - such as asset conversion - poses a vulnerability to the security of cyber criminals. When solely looked at the physical surroundings of cyber criminals in the Netherlands, this study concluded that cyber criminals who are located in a high-risk area opt for limited territorial control. Their micro external zone, which is visible from the outside for potential threat agents, have to blend in into their direct physical surroundings. Conversely, target hardening is more apparent in their micro internal security zone in which the operations room is located. Two of these physical security mechanisms stuck out of the research data: access control and surveillance. Besides such physical protective objects of a defensive nature, multiple occasions have been observed in which the referent object him/herself applied the offensive countermeasure of violence against threat agents for security purposes. Lastly, this chapter ends by briefly summing up some of the vulnerabilities of the observed deviant physical security standards. Further work needs to be done to establish whether there are differences in physical security between high-risk and low-risk points of attack origin, and differences between motives, age and computer-focused and computer-assisted criminals. Which IT and non-IT focused objects are found in which spaces? Are there differences in hiding passage usage between profit-driven computer-focused criminals and sexually-driven computer-assisted criminals? The data to conduct such statistical research is available. LEA generally maps on which specific location what evidence was found, and the findings may improve the search competencies of legal practitioners.

Chapter 8

Investigative Responses Against Deviant Security

While this study acknowledges that the regulatory toolbox of Internet governance to confront cyber crime goes beyond law-enforcement [606][607, p.502][608][609], the legal end of this study aims at producing outcomes that benefits legal practitioners from the cyber security community who work on public policy, legislation and especially investigations on profit-driven computer-focused crimes. This occupational group nowadays includes many professionals with a technical background such as data scientists, digital investigators and software developers. Based on the findings of the previous chapter and empirical evidence, and taking into account the general standpoints of the human rights-driven multistakeholder approaches against cyber crime of the International Cyber Strategy and the National Cyber Security Strategy 2 of the government of the Netherlands, and an underlying study of The Netherlands Scientific Council for Government Policy [564][610][611], suggestions for investigative approaches have been developed for the Dutch National High Tech Crime Unit and implemented by the Central and Regional Criminal Investigations Divisions of the Dutch national police. The suggested approaches as presented in this study are further refined by reviewing i) four investigations that actively applied the suggested approach of Section 8.2 in practice, ii) an independent process evaluation of such an investigation [415], iii) numerous investigations that did not apply the approach in practice, and iv) the No More Ransom Project - an award-winning cross-sector platform against ransomware.

Good guy security against the commission of crime, and bad guy security against police investigations, are cat and mouse games with all key players constantly improving, innovating and implementing lessons learned, while having good reasons to hide their capabilities [612][102][317, pp.288-289]. The paradox is that both sides - law-breaking and law-abiding entities - may strive for perfect security which is an illusion as described in Sections 2.3.2, 2.3.3 and 5.2, and may end up with insecurities and/or decreasing security for themselves and others [58][612]. Any investigative approach against DevSec should therefore aim at reducing the double whammy effect of deviant security, while avoiding erosion of public security because of e.g., securitization and commodification. The overall vision as laid down in this chapter is that police investigations on cyber crime should evolve around different notions of security. More specifically, investigations should be understood as security-driven means that breach deviant security and affect the criminal's CIA triad to provide human security. Within this normative framework, investigations on profit-driven computer-focused crimes should transform into a public service model and work towards multiple outcomes that go beyond attribution of offenders for prosecution purposes. This study further provides empirical evidence how deviant security affects the current global investigation system, and argues that technical harmonization between law-enforcement agencies of democratic states governed by the rule of law might be a fix for that problem. Lastly, this chapter zooms in what kind of investigations should target which types of cyber criminals, and concludes that proactive public-public investigations should focus on 'protection providers', while reactive public-private investigations should aim at 'commission providers' and autarkic cyber criminal organizations. In other words, this chapter elaborates on cyber security for whom, from what and by what means [72]. The suggested approaches further take notice of the underlying problems that cause the current effectiveness crisis in investigations.

8.1 Security-Driven Investigations That Provide Human Security

No doubt, most, if not all, law-enforcement agencies will proclaim that their investigations contribute to the security of law-abiding referent objects by preventing, deterring, detecting and correcting those who commit crime. However, are these law-abiding referent objects defined by the border-centric view on cyber security and cyber crimes, or by the borderless view on cyber security and cyber crimes as described in Section 2.3? More specifically, should investigations on cyber crime solely contribute to national security, or to a broader, richer concept of security? While this section predominantly discusses *normative aspects* of investigations that go beyond national interests, the next Sections 8.2 and 8.3 provide arguments for the many *practical reasons* why investigations should not be solely based on national interests. Albeit far from perfect, criminal justice systems of liberal democracies, including police investigations, are best equipped to ensure the equitable distribution of security as a basic public good and positive presence for *all* individual Internet users, i.e., human security, not merely for citizens within specific national borders. Yet the goal of this rich security concept is threatened by both the cyber criminal and the cyber security communities. To protect investigations against attacks from both communities, government actions against cyber crime have to become security-driven. Thus, investigations are security-driven tools that breach deviant security to provide human security. These notions outline the normative framework - the core principles and prerequisites - in which the other investigative concepts of the next sections have to be viewed and tested against.

Investigations to provide human security & Internet as a global public good On the one hand, investigations in the Netherlands and elsewhere are hardwired to national interest. They are enshrined in national law, and can generally only be launched when crimes are committed within the territorial jurisdiction of the state, or in other words, when national interests are violated. On the other hand, Dutch governmental policy documents postulate that cyber security - read: investigations - should protect universal interests such as fundamental rights, freedoms and values. Given the transnational nature of cyberspace in general and glocalized nature of deviant security specifically, safeguarding these interests has nowadays indeed an international dimension [564, pp.2-3]. Bringing together national, international and universal aspects of investigations on cyber crime is a challenge, yet possible when legal practitioners aim at providing i) *human security* and ii) regard the Internet as a *global public good* - two academic concepts that both fit within the borderless view on cyber security and cyber crimes.

Human security puts the individual - read: citizens - at the receiving end of all security concerns [613][318][37], and has a 'clear resonance with the historical, continental European understanding of policing as integral to ideas of good governance, the condition of order in the community, and the prerequisites to good order' [31], and 'the primacy of human rights, clear political authority, multilateralism, a bottom-up approach, regional focus, the use of legal instruments, and the appropriate use of force' [614]. In other words, what is 'best' for the state is, by definition, best for individual citizens [72, p.50], including for those who may have trespassed substantive law. As Section 5.3 explains, public security is a non-excludable and non-rivalrous good that in many instances also must protect suspects of crime. As human security is deliberately loosely defined and may even encompass threats to the environment or human dignity, this study follows a more narrow concept of human security that focuses upon violent threats to individuals and threats to their property [613][615][31]. More specifically, Dunn Cavelty's concept of human-centric information ethics is helpful for applying human security in cyberspace. These ethics evolve around a common ground for all stakeholders - namely, vulnerabilities - and include human beings as well as non-human and non-individual entities [97, pp.710-712].

Translating human-centric information ethics to the world in which legal practitioners operate means that the fruits of investigations on profit-driven computer-focused crimes should be an inclusive public good which *all* citizens should be able to enjoy [98], and not as a private commodity that only a happy few can afford [31]. Law-enforcement agencies of liberal democracies should take the findings of Section 7.3 into account that a single offender can distribute his/her victims all over the world. Many of these victims cannot rely on basic state protection while, controversially, some offenders can. In other words, related police investigations should consider its global impact on the physical and psychological integrity of all human beings, and those artificial and distributed entities that affect these citizens such as the integrity of the financial system. The implication of this proposition is that legal practitioners should regard and respect the Internet's core as a non-excludable and non-rivalrous global public good that provides benefits to everyone in the world [611]. Cyber security restricted to physical national borders is in today's technically, economically and socially networked societies of the Information Age not only impossible, but will especially harm citizens in low-risk points of attack occurrence as explained in Table 7.2. As sociologist Broeders states: 'an open Internet is so beneficial to countries with an open economy and international outlook that it should be considered an "extended national interest"'. Therefore, this study argues that investigations must indeed find 'areas where national interests align with strategic global issues that can be defined as global public goods' as well [611, p.42]. Strong encryption technologies are such a global public good. While some governments - like the Netherlands [616] - reject the idea of backdoors, this study also shows that Dutch law-enforcement agencies have successfully bypassed the deviant usage of encryption during investigations on DevSec providers, largely by exploiting other vulnerabilities in MOs. Based on the findings of the previous chapters, we now understand why these weaknesses occur on a meso and micro level. A few niche facilitators become too central (read: successful) in the underground and miss the intangible (e.g., knowledge) assets to correctly implement dual-use encryption products. This is understandable: the added value of most DevSec providers lies in additional technical computer security controls of an administrative nature such as deception and distribution as countermeasures.

Although human security acknowledges that many actors - including the individual - may provide security, it regards the state as the entity that is most capable to guarantee security to citizens [318]. In other words, human security is state-led protection with programs, like investigations, aimed at empowering all people to secure their own interests [31]. Yet investigations that protect the Internet as a global public good are also means of Internet governance for which the Dutch government favors a multistakeholder model [611, pp.16, 33]. Taking this position into account, this study continues by explaining in the next paragraphs and sections how such a multistakeholder approach can also be applied in investigations on computer-focused crimes to protect Internet as a global public good. Such investigations should further ensure the state's public mandate to restore human security by means of investigations and help those who are in need of help and/or prosecuting suspects.

The provision of human security and Internet as a global public good in practice Ransomware affects both the systems of vital infrastructures as well as of citizens around the world. The No More Ransom Project is a great example that the provision of human security and Internet as a global public good in cyberspace is very much possible. This initiative of the Dutch NHTCU, Europol and two AV vendors offers over 50 free decryption tools against more than 100 types of ransomware to victims all around the world, and explains to the general public in over 25 languages how to prevent becoming a victim. The website further explains the importance of filing victim complaints and forwards victims to their applicable national police force. Similarly, the No More DDoS Project of the Dutch NHTCU detects and takes down DDoS booters, regardless which country, victims and/or networks are affected most. When young Dutch clients of these services are identified, the Hack_Right initiative - a consortium of Dutch law-enforcement and child protection agencies and several universities - will execute alternative sentences for these vulnerable suspects with more emphasis on deterrence, rehabilitation, restitution and restorative justice [617].

Security-driven investigations against multiple threats When discussing the concept of human security, scholars stress the importance of democracy, rule of law and respect for human rights [614][618]. This means that 'if the pursuit of security [by the cyber security community] comes at the expense of human rights, then not only is the quality of that security compromised, but the very principles of democracy are threatened' [31]. As Sections 5.3 and 6.2 show, authoritarian regimes provide state security to their home-grown cyber criminals, while corruption within the security apparatus of e.g., weak democratic states makes state protection a private commodity for those who trespass substantive law. Ultimately, liberal democracies governed by the rule of law are best equipped to deal with both threat agents - i.e., cyber criminal and cyber security communities - and promote, provide and restore the public good of human security [98]. While the Dutch government uses similar language in its International Cyber Strategy and emphasizes that security and freedom are complementary rather than conflicting interests in cyberspace [564], it is so far unclear how to provide human security in practice by means of investigations. Based on the findings of the previous chapters, a first step forward is by making cyber crime investigations *security-driven*. This means that states need to install a variety of administrative, physical and technical security measures that are able to simultaneously protect investigations on cyber crime from i) conduct of the cyber security community that harms citizens, ii) offensive countermeasures of cyber criminals for deviant security purposes and iii) other states for reasons of national security.

Investigations protected from conduct of the cyber security community that harms citizens Let us begin with the first and main concern of the borderless perspective on cyber security and cyber crime, and for which this study provides proof: citizens are indeed threatened in their security by - amongst others - geopolitical and financial incentives of the larger public and private cyber security community. Additionally, law, policy and investigations hold the ability, according to criminologist David Wall, to unleash 'an uncontrollable drift [...] to a control society where post-event [...] policing models will be replaced by a ‘pre-crime’ mentality based upon simulations of crime and behavioral predication’ [262, p.202]. Indeed, law-enforcement agencies that are subjected to democratic scrutiny and constitutional control have administrative accountability mechanisms installed to protect citizens. These mechanisms hold both individual police officers, as well as complete organizations, responsible for effectively delivering basic services of crime control and maintaining order, while treating individuals fairly and within the bounds of law. Yet the findings of this study raise the question if these traditional mechanisms are sufficient for today’s challenges, and provide additional arguments why, as legal scholar Bert-Jaap Koops states, we have ‘to rethink the legal protection of citizens in the form of new checks and balances in the criminal legal system’ [619, pp.358-359]. As explained in Section 6.4 and throughout Chapter 7, today’s challenges include the impact of the distributed, glocalized and intertwined nature of deviant security on transnational investigative collaborations. Investigations are propelled by decisions in other countries [620, p.42], while many investigative efforts will not be scrutinized by the judiciary of the countries involved when suspects are not identified and brought to court. These and other problems associated with cyber crime investigations undermine fundamental legal principles such as mutual recognition of judicial decisions and police accountability in criminal matters (see [621]). Many of the vulnerabilities of cyber criminal MOs can be exploited by the collection, analysis and usage of large data sets by means of ‘intelligent forensics’ [622][504, pp.26-27][623, pp.224-225], like artificial intelligence techniques, natural language processing or social network analyses. Yet legal principles that are associated with the collection of evidence, such as data minimization, seem disconnected with the realities of today’s cyber criminal underground. These disconnections are best explained by - amongst others [624, p.256] - the economics of deviant security. Data minimization for LEA is near to impossible when cyber criminals themselves apply data maximization (a deception tactic, see Section 6.5), and outsource their security to centralized providers with automated business processes and large historical client databases who keep law-abiding outsiders at a distance (see Sections 6.1 and 7.3). A shift to regulating analysis and usage of such large data sets for investigative purposes - called algorithmic accountability [625] - is absent [626, pp.19-20], although Dutch courts have reviewed the outputs of such intelligent forensics and concluded that these techniques are allowed for investigations [627]. While the latter applies to accountability of quantitative methods of working in investigations, many existing traditional accountability mechanisms supervise the qualitative investigative methods in which the police investigator him/herself is the main instrument to collect, analyze and use evidence. Fortunately, these accountability mechanisms like complaints procedures, evaluation, monitoring and transparency also reveal the human vulnerabilities in police organizations that cyber criminal organizations try to exploit such as bribing and/or threatening LEA officers.

Investigations protected from offensive countermeasures of criminals and states This brings us to the second issue of securing investigations against attacks from cyber criminals that is discussed in, for example, Sections 5.1 and 7.4. The confidentiality, availability and integrity of evidence - i.e., evidence security [628] - must be ensured at every investigative phase [629]. Security-driven in this regard does not only mean investments in administrative security measures to avoid human vulnerabilities, but also ensuring appropriate technical and physical measures against other offensive attacks by cyber criminals for DevSec purposes. Besides preventing computer-focused crimes against law-enforcement agencies - such as the hack of Anonymous on a conference call between law-enforcement officers [630], or DDoS attacks on a police website with evidence about a case after a request for public assistance - there is also a need to install physical security procedures for police officers. As this study shows, cyber criminals take physical countermeasures of a defensive and offensive nature to protect their criminal assets, while turned on IT-focused objects - hardware like a laptop - might be more important to an investigation than physical subjects like an arrested suspect. Based on the findings of Section 6.4, law-enforcement agencies should further increase the information asymmetry that cyber criminals face about who these legal practitioners are and how they execute their investigative powers, including their security-driven investigative approach and capabilities.

Lastly, LEA should be aware that their investigations might become targets of intelligence agencies and/or national politics. As shown in Section 7.3, cyber crime has become a ball in a game of power geopolitics in an increasingly multipolar world, and as such, states can be intentional deviant security providers to cyber criminals. This means that legal practitioners should receive appropriate training and procedures to understand and effectively deal with this particular threat. Besides making investigations security-driven, other means to provide human security through police investigations are discussed in the next sections.

8.2 Investigations as a Public Service With Multiple Outcomes

While many academic and policy papers discuss the need for public-private partnerships on Internet governance in general or against cyber crime in particular [631][149][35][632][85][564][610], few zoom in how operational public-private investigations on profit-driven computer-focused crimes (ought to) work in practice outside the US [72][633]. This section argues that these investigations should be modeled as a public service model within public-private alliances, and aim at i) damage mitigation for potential victims, ii) assistance of actual victims, iii) disruption of the cyber criminal process and iv) attribution for prosecution and alternative sanctions. Each of these goals will also limit confidentiality, integrity and availability and related attributes of deviant security, and as such harm assets of cyber criminals.

Investigations as a public service within alliances Joining forces with key players in the public and private sector will help law-enforcement agencies to have added value in the larger cyber security value chain. Investigations should become a *public service* within operational *public-private partnerships* (also known as multi-agency cross sector partnerships [34]). The idea of investigations as a public service is a practical implementation of the concept of *nodal governance*: the acceptance that the monopoly of the state as the sole provider of security is not a durable condition and that policing has become plural in the sense that various actors play a role in policing cyberspace [634][635]. During this study, many starts of and breakthroughs in investigations were the result of private and public partners. It is therefore vital that police intelligence and evidence can be shared with, and external specialists can be brought in from, a range of public and private third parties for academic, compliance, intelligence and investigative purposes (as arranged in e.g., articles 16 to 24 of the Dutch Police Data Act).

Why work with law-enforcement agencies (or private partners)?
While most key players in the cyber security community are only allowed to take defensive countermeasures, LEA as mandated breachers have a monopoly on launching offensive countermeasure against cyber criminals, i.e., exploit vulnerabilities in cyber criminal MOs to collect unique data. These investigative methods and techniques breach intangible and tangible protective assets of cyber criminals to collect criminal tangible and intangible assets, and includes seizure of IT and non-IT related physical objects, interrogation and interviewing of physical subjects, lawful intercept of information capital in motion and preservation of information capital at rest, and the collection of metadata like subscriber and payment details, netflow and the like. Other key players need the outputs of these investigative means - e.g., malware samples, IoCs, TTPs, and the like - to increase their security against cyber criminal attacks. This study identifies at least four incentives why it is beneficial for public and private parties to closely collaborate in alliances, and how the double whammy effect of DevSec is reduced as a result. The first benefit is *cost reduction* as scare public resources are more efficiently deployed, less work has to be conducted by each party and any additional expenses are shared. Victims save costs as well as data collected by offensive countermeasures may greatly shorten the research time of private security researchers. Secondly, public-private partnerships will lead to *product improvement* as the use of additional data, tools and competencies will increase the quality of investigations. Thirdly, PPP may lead to a *reputation boost* for LEA among the general public, (victim) witnesses and other key players as more effective results are achieved. Hopefully, these positive messages sustain and restore trust in government actions, have a general preventive effect and help victims of cyber crime to come forward and file a complaint. A last incentive is *customer acquisition.* In multiple instances, other private agencies shared evidence about advanced computer-focused crimes with, and offered their services to, the NHTCU after media outlets reported about successful public-private partnerships.

Section 7.1 explains why the reversed electronic panopticon forms a major vulnerability to cyber criminals. Based on this finding, far-reaching investigative collaborations with non-profit organizations, public agencies and the private (security) industry are vital to exploit this weakness and put together the pieces about who did what. Key players hold unique intelligence, evidence and insights that will help LEA to overcome the information asymmetry of Section 6.4 about cyber criminals and their crimes. Such partnerships allow national law-enforcement agencies to specialize and thus only do what they do best instead conducting all the investigative work from A to Z themselves. In practice, it is hard for LEA to beat AV vendors in malware analyses; CERTs are better in notifying victims and distributing threat analyses to potential victims; and private digital forensic services are preferred by victims to research their infected systems over public agencies. In several of the reviewed operational public-private collaborations, each partner collected, shared and analyzed operational data, and provided specialized services to the investigation. So these horizontal partnerships can more specifically be characterized as *public-private alliances*, ranging from one-off, unilateral acts to structural collaborations that are formally enacted by legal contracts and legal persons (such as the Dutch ECTF and US NCFTA) [415, pp.9-10, 19]. Although law-enforcement agencies outsource parts of their investigation to third partners, public-private investigations are conducted within the appropriate public legal frameworks and under the supervision of the relevant public authorities, including the judiciary. Moreover, that public and private organizations become increasingly equal partners does not mean they serve equal legal and ethical interests as shown in Figure 8.1 (see also [72, pp.54-55]). Public interest must prevail over private interests, hence the term investigations-as-a-public-service. In the reviewed investigations, the NHTCU aimed at finding horizontal, non-hierarchical arrangements and 'win-win situations' by consensual decision-making (see text box above), but always had the leading role in alliances [636]. Besides the legal monopoly on offensive, technically advanced and evasive means of data gathering of law-enforcement agencies, officers were also organizationally and technically in the lead during the observed public-private investigations. Private parties generally accepted their subordinate role in these operations. They have to: obstruction of police investigations is a crime under Dutch Penal Code for both legal and natural persons.

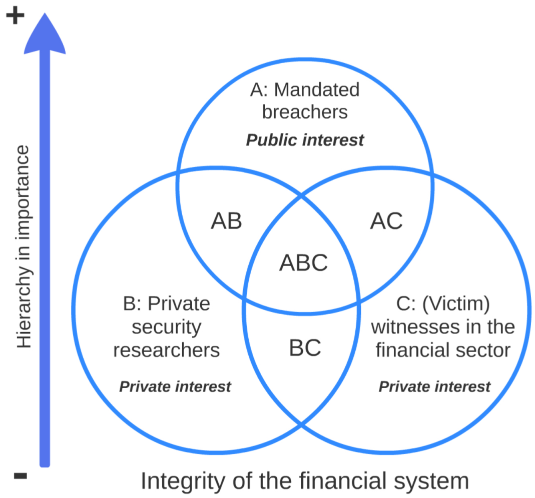

+
Hierarchy in importance
-
A: Mandated breachers
Public interest
AB
AC
ABC
B: Private security researchers
Private interest
BC
C: (Victim) witnesses in the financial sector
Private interest
Integrity of the financial system

Figure 8.1: In investigations on profit-driven attacks against financial institutions, both public and private interests contribute to the integrity of the financial system. In situation BC, the private security industry (read: contracted security) closely collaborates with (read: in-house security of) private financial institutions by helping to increase their protection against threats and/or clean infected systems. Especially when the nature and extent of threats and attacks on financial systems are persistent and severe, the integrity of the financial system is also very much a public affair. The private security industry and private financial sector, together with mandated breachers and other public agencies, than very much serve a public interest that prevails over any private interests (situation ABC).

A multistakeholder approach with multiple outcomes The next step is that law-enforcement agencies combine, manage and supervise the combined data set, i.e., the information collected by the offensive countermeasures of investigations and the data collected through defensive countermeasures from other key players. The big question is which products law-enforcement agencies can extract from these enriched data sets. Traditionally, investigations are deployed for attribution only - namely: who did what for prosecution purposes - and has few possible outcomes that go beyond punitive sentencing. Because points of attack origin, linkage and occurrence may not be located in the same jurisdiction, and perpetrators frequently operate from safe havens, bringing suspects to justice can take several years and is in many instances even impossible. Therefore, LEA should explore additional outcomes and related outputs that go beyond attribution. Indeed, attribution for prosecution purposes is inextricably linked to *repression of crime*. Opposite to repression is *prevention of crime*. However, prevention and repression of crime do not form a dichotomy in this study's investigative approach, but are rather two ends of the same continuum. As Figure 8.2 depicts, four outcomes and related outputs can be derived from these investigative data sets that go from prevention to repression of cyber crime. The central idea behind this approach is that law-enforcement agencies should affect intangible and tangible commission and protection assets of cyber criminals by deploying their monopoly on offensive investigative powers, exploiting their unique information position and serving a wide audience of stakeholders, most notably citizens.

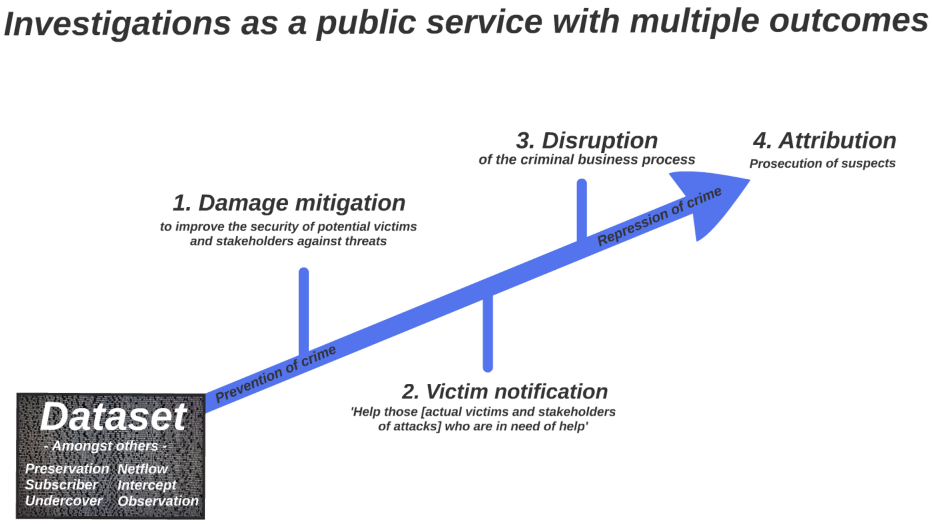

Investigations as a public service with multiple outcomes
3. Disruption
of the criminal business process
4. Attribution
Prosecution of suspects
1. Damage mitigation
to improve the security of potential victims
and stakeholders against threats
Repression of crime
Prevention of crime
2. Victim notification
'Help those [actual victims and stakeholders
of attacks] who are in need of help'
Dataset
- Amongst others -
Preservation
Netflow
Subscriber
Intercept
Undercover
Observation

Figure 8.2: There are two victim-based and two offender-based outcomes in the approach that can be achieved by collaborating with and serving as many Internet governance stakeholders as possible.

1. The first and most preventive outcome is *damage mitigation*. Police investigations may generate data about crimes that are still in the preparation and pre-activity phase. Moreover, data may also be available about ongoing crimes in the activity or post-activity phase that are about to target other industries or jurisdictions in the imminent future. In both situations, there is a need for key players in the cyber security community to be aware about these threats. Mitigation is focused on helping these stakeholders to increase their security against cyber criminal threats before they turn into successful attacks. As such, harm to systems will be limited or even prevented. In other words, damage mitigation aims at generating actionable cyber threat intelligence for a range of public and private actors, and as a consequence, reduce the effectiveness and conversion rate of future attacks on potential victims. Related outputs and audiences include warnings in media outlets for the general public, threat analyses for private industries, and actionable insights for potentially vulnerable individuals, groups and organizations about upcoming attacks. Damage mitigation limits the confidentiality, and related attributes of undetectability and unobservability,

of criminal assets like MOs.

2. Next follows a key task of many law-enforcement agencies, and prescribed in article 3 of the Dutch Police Act 2012: give help to those who are in need of help, i.e., *victim assistance*. During investigations, LEA may discover victims in e.g., the system of a C&C server. Incoming bots and stolen company and personal data on such servers are not only assets to criminals, but also to their lawful owners. This particular outcome does not focus on potential victims and threats, but *actual* victims and past and ongoing attacks. In such a situation, victims are detected, identified and subsequently notified about their victimization and MOs. Help is being offered to stop the attacks and/or further damage to systems, software and personal and company data, including blocking of credit cards. Victim assistance limits the availability of criminals assets such as infected machines.

These victim-based approaches - damage mitigation and victim assistance - affect many cyber criminal assets related to crimes (as compared to the criminal). The role of the police in this approach is supporting multistakeholders like CERTs and other key players of vital infrastructures in their responsibilities to ensure that networks and users are safe and secure, thus promote human security and the Internet's core as a global public good.

3. This study further argues that investigative powers are always disruptive to MOs, even when not put in action as even the mere threat of investigations affect the cyber criminal business process. So, after the previous two victim-based approaches comes the first offender-based approach of *disruption* of modus operandi as defined by this study. In other words, hindering the processes of committing crime and protecting crime and the criminal. Outputs and interventions should go beyond existing interventions that aim at skimming profits of the commission of crime such as seizing financial assets like hard cash or cryptocurrencies. Disruption may not only consist of increasing the commission costs [382], but also the total costs related to protection such as taking down vital criminal servers or adding false positives into the cyber criminal process. In such cases, cyber criminals will either over spend on security or under protect assets. Other disruptive interventions may focus on bringing either collective underground economies or individual MOs to a suboptimal level by respectively promoting market failures via increase of information asymmetries [637], or disturbing the balance between commission and protection via e.g., targeted messages to individual suspects to act in a particular way or omit certain behavior (as compared to elevated media attention after takedowns of cryptomarkets that seems to increase drugs trade [638]). Disruptive interventions like seizure of stolen money limits the availability of criminals assets, while false positives affect the integrity of assets and direct messages to cyber criminals affect the assets' confidentiality.

4. The last and most repressive goal of investigations is *attribution* for prosecution purposes and alternative sanctions. An important remark is that prevention of potential offenders as a primary goal of investigations has no place on the continuum. Investigations differ from supervision of compliance, and exclusively deal with suspects and violations of substantive law as compared to behavior of high-risk but still law-abiding groups. Indeed, repressive punishments may hold general and specific deterrent effects. They send respectively an important message to the general public, and help to avoid reoffending by the suspect and further damage inflicted to victims. Nevertheless, many alternative sentences - e.g., community services, financial transactions, fines, official warnings and probation - for low-threat offenders such as young offenders hold punitive effects, and are therefore primarily forms of repressive punishments. Yet these sanctions are less far-reaching than incapacitation, with more emphasis on other goals of punishments such as the previously mentioned deterrence, and rehabilitation, restitution and restorative justice. Public verdicts limit the confidentiality of criminal assets, incarceration limits the availability of the criminal, while the overall truth-seeking process sheds light on who did what, thus limits deception and increases the integrity - i.e., accountability, authenticity and non-repudiation - of who did what.

These last two offender-based approaches damage assets related to the criminal and his/her crimes. The latter harm is of course to the physical subject of the criminal in case of an arrest, while disruption damages tangible non-IT objects include seized cash money and intangible assets include lowering of the status and/or reputation of a member in the cyber criminal community.

The snowball effect of a multistakeholder approach with multiple outcomes
In practice, these multiple outcomes do not only stand on their own, but are also communicating vessels and can be executed in a linear fashion. During an investigation of a cyber criminal advanced persistent threat (APT), private security researchers started by writing a threat analysis for financial institutes about the observed attack based on preserved C&Cs. The report contained many IoCs and was distributed by the Dutch CERT to other national CERTs that subsequently sent the report to the associated members of their national financial Information Sharing and Analysis Centres (FI-ISACs). This allowed banks to take necessary countermeasures against the threat. Based on the enclosed IoCs and TTP, some financial institutes discovered that they were not potential but actual victims, and requested the assistance of the private security company that wrote the report. Other actual victims were discovered through analysis of the incoming bots of the C&C servers, and were notified by their national CERT. Identifying the victims and helping to remove the infections before financial harm was done does not only assist victims but is also disruptive: the cyber criminal made upfront investment costs to infect and monitor the machines, but did not yield any profits yet. A suspect was in sight during the execution of these interventions, yet this did not harm the attribution process. There might be a pattern in this: many cyber criminals do not necessarily stop their criminal activities after LEA interventions. During an operation against ransomware, the Dutch police and a private security company offered the decryption keys to victims for free. Yet the suspects continued their activities even after they keys were published. They were forced to alter their MO to a suboptimal level in which new mistakes, failures and vulnerabilities occurred that provided further evidence against them.

8.3 Technical Harmonization for a Global Investigation System

While the previous section focuses on public-private investigations, the current section describes global public-public investigations. Firstly, the current global investigation system is explained, and how deviant security practices thwart this informal and unwritten system that is based on information economics. As Figure 8.3 depicts, four stages of international collaboration are subsequently identified, resulting in the conclusion that investigations have to go beyond national interest and move towards technical harmonization between law-enforcement agencies of democratic states governed by the rule of law.

'Hellooo, I am a botnet operator! Does anybody hear me?!'
During this study, the Dutch National High Tech Crime Unit identified a botnet operator who did not take many precautions to hide his true identity and malicious activities. Still, this criminal remained active for years, while a private non-profit researcher continuously provided public updates about the botnet C&Cs. Apparently, national police organizations had more incentives *not* to start an investigation on the botnet, than incentives to start an investigation against the botnet. Based on the intelligence about the botnet and the findings of this study, a questionnaire - including a case study - was developed for the EU Policy Cycle EMPACT on cyber crime 2013 (European Multidisciplinary Platform Against Criminal Threats). The questionnaire focused on what the incentives are that trigger team leaders and case agents of national cyber crime units to initiate an investigation on a botnet. The subsequent case study presented nineteen characteristics related to the botnet operator (e.g., true identity known but located in a country affected by the Arab Spring), technical infrastructure (e.g., multiple C&Cs that rotate every few months, hosted in over 40 countries) and victims (e.g., number and total damage unknown). 25 team leaders and case agents from Asia, Europe and the United States, filled in the questionnaire. The results of the questionnaire were afterwards presented to and discussed by the heads of the EU national cyber crime units in 2014 and summarized in Table 8.1.

The current global investigation system If cyber criminals, infrastructure and victims are distributed as a countermeasure, then surely law-enforcement agencies must respond in an effective, global manner. However, no official transnational response system exists today that prescribes which country has to take that very important first step to start an investigation of transnational cyber crimes. This is left to individual countries to decide for themselves. The initiative to investigate a transnational cyber crime is predominantly a national affair as police organizations are organized within sovereign states and must serve national interests. For this reason, it is unlikely that country X will start the investigation and/or takedown of a botnet of which the majority of infrastructure, victims and perpetrators are based in country Y. However, it could be argued that there exists an unwritten and informal response system that deals with transnational cyber crimes and is based on information economics. National police organizations have specific *incentives* - i.e., violations of national interests - that trigger them to start an investigation of transnational cyber crimes. Countries that initiate such investigations are, for example, disproportionally affected by the crime in terms of victims or misused infrastructure.

As the investigation progresses, this initiating country cooperates with other affected countries on the basis of mutual legal assistance treaties (MLATs) or joint investigation teams (JITs) in time. In the Bredolab botnet case, the operator did not apply distribution as a deviant countermeasure. Because virtually all C&Cs were continuously hosted in the Netherlands, centralization and location-boundedness and time-boundedness worked as a vulnerability. As a result, the botnet became too noticeable to the outside world. Subsequently, the Dutch NHTCU started an investigation with a private partner on this botnet and subsequently exploited its vulnerabilities. As the investigation progressed, the NHTCU collaborated with the Armenian police who arrested the operator of the botnet. In other words, one country felt responsible to start an investigation, because their national interest was evidently violated for a considerable time. Other countries responded as well, but only after the initiator of the investigation - i.e., the Dutch NHTCU - officially requested to cooperate. Still, the majority of affected countries – notably, victims of the Bredolab botnet were located all over the world – were *free riders*. They benefitted of the initiative of the Dutch NHCTU and cooperation of the Armenian police, without making any contribution or paying the costs of this benefit. The current global investigation system, however, has no problem with these free riders: it is expected that when these countries are heavily affected by another botnet (in other words, have an incentive), they will take the initiative to start an investigation themselves. In such a situation, other (previously initiating) countries will benefit and become free riders themselves.

'See you in court'
While the emphasis in this section is on DevSec practices that thwart the start of an investigation, countermeasures of cyber criminals resonate till the very end of the postactivity phase of an MO, namely during court proceedings. Besides the predicted shift from primary evidence to corroborating evidence [20, p.393], prosecutors face other challenges as well. According to legal practitioner participants during this study, evidence is collected and presented as such that suspects are forced to make 'concrete, more or less testable, not a priori unlikely statements'. Yet DevSec is focused on avoiding verification by hiding the real and showing the false, and minimizing linkability by e.g., distributing entities. As a consequence, legal defenses consist of - amongst other things - respectively drawing alternative scenarios and pointing towards loose ends in investigations that might provide *ex culpa* evidence. These tactics place a heavy burden on police investigators who have to go back and find answers, in some occasions even years after they sent the dossier to court.

Deviant security affects the current global investigation system However, the informal response system not only fails when cyber criminals, misused infrastructure and/or small or low-impact multiple victimizations are distributed among many jurisdictions, a legal problem known as *de minimis non curat lex* [34][80, p.91]. Other deviant security practices, such as deception, secure-deletion and encryption, have taken a flight as well, making it difficult to determine the identity of perpetrators and victims in the preparatory investigative phase. Especially the latter two are important incentives for deciding to precede to an official investigation which allows the deployment of more evasive investigative powers. To conclude, today's deviant security practices effectively take away the incentives of countries to start an investigation. Still, every country – unconsciously – expects that other countries will take the initiative.

All respondents (N=25) indicated that they would *not* start an investigation against the botnet of the case study. The botnet administrator made sure that no country felt the responsibility to start an investigation, because his deviant security practices gave them no incentive to do so. The incentive problem affects both individual countries and the collaboration between countries. Thus, initiatives focused on tackling the incentive problem should function on both a national and international level.

The four most important incentives of 25 managers and case agents of cyber units to start an investigation on botnets	**Related DevSec practices that affect the incentives to start an investigation on botnets**
✓ 'Indications that the perpetrator or his henchmen are residing in your country.'	✗ Botnet herders operate from low-risk points of attack origin and apply a range of countermeasures to protect their identity, such as deception tactics for security purposes.
✓ 'The expectation that you will work with trusted private companies or foreign public agencies that are willing to cooperate.'	✗ The cyber security community is intertwined with the cyber criminal community; public and private agencies can be DevSec providers; and the increasingly multipolar world works as a countermeasure for cyber criminals.
✓ 'Indications of considerable amount of damage or high value targets in your country.'	✗ Victims are distributed among many points of attack occurrence, have relatively little damage, and barely file complaints and as such are not visible for LEA.
✓ 'Indications that a considerable amount of C&C servers are hosted in your country or for a considerable amount of time.'	✗ C&C servers are continuously extended, dispersed, replaced and rotated among multiple points of attack linkage.

Table 8.1: Prior to the questionnaire, 24 incentives related to victims, infrastructure, cyber criminals and the cyber security community itself were identified based on interviews and observations. These incentives were included in the questionnaire and presented to managers and case agents of various cyber units in Asia, Europe and the United States. They could rate these incentives on a scale of five options ranging from Not at all important, to Very important, including the option No opinion. The above left four incentives were mentioned by the respondents as the most important incentives to start an investigation on botnets.

Four stages of international collaboration International collaboration is an important means to deal with deviant security practices that affect today's global investigation system. This study argues that international investigative collaboration against cyber crime progresses through four stages (see Figure 8.3). On the most basic level, governments first have to *acknowledge* *each others strategic importance* for their national interests in cyberspace on an administrative and/or political level. The output of such contacts are threefold, and might be set in formal documents like memoranda of understanding (MoU). Firstly, agreements are made on a policy level, such as organizing periodic meetings, sharing best practices on investigations or simply being present on international conferences hosted by the other party. Secondly, acknowledgement of strategic importance includes agreements made on an operational level. Thus, even countries that cannot legally or politically conduct joint investigations or share investigative information with other nations are still able to make agreements about fighting domestic points of attack that are a problem to the other party. Lastly, nations can make agreements to work towards the next step in international collaboration: *legal harmonization/unification.* Before parties can share investigative data and/or conduct joint investigations, relevant substantive and procedural laws and data protection acts have to be harmonized. Legal harmonization of cyber crime laws occurs on both a bilateral and multilateral level of which the Council of Europe's Cyber Crime Convention is the most far-reaching international treaty on cyber crime [82, p.215]. Legal harmonization and unification paves the way to closely collaborate on investigations through MLATs, JITs and dedicated cyber crime police liaison officers. As such, the next phase is *operational alignment* between partners as there is a need to coordinate and even converge investigations against transnational cyber crimes. The coordination between the US FBI, a German *Landeskriminalamt* (LKA), Dutch NHTCU and Europol of the takeover and takedown of the two largest cryptomarkets is a great example. While Alphabay was shut down by the FBI, the Dutch NHTCU had Hansa already under control. The latter market was subsequently flooded with so-called 'Alphabay refugees' that had to find a new secure marketplace. The current last step in international collaboration is *organizational integration* in which various agencies come together at a single physical location (and increasingly online environments as well) to investigate crime, share and analyze evidence and/or execute a joint operation as happened during operation BlackShades [414]. Examples of such international law-enforcement platforms are INTERPOL's IGCI (that houses INTERPOL's Global Cybercrime Programme), Eurojust, Europol's EC3 and JCAT initiative, and public-private working groups, partnerships and even mailing lists like national ISACs, the US NCFTA, the Dutch ECTF and various ad-hoc consortia against specific malwares.

As shown in the previous paragraph, deviant security controls easily play out any assessment based on national interests whether to start an investigation or not, while Section 7.3 describes the digital divide between different but interconnected cyber security blocs. These international initiatives do a great job in overcoming the incentive problem by bringing together parties with different security goals, and the digital divide by means of capacity building [364, pp.7-8]. They also prove invaluable in solving the subsequent organizational and legal issues that public and private agencies face when jointly fighting cyber crime, and thus integrating all the previous steps in transnational collaboration. Despite inherent challenges of sharing intelligence and evidence between non-trusted parties [639], governments and law-enforcement agencies should further make an effort to overcome geopolitical barriers and search for common interests with other governments and public and private agencies to turn low-risk areas for cyber criminals into high-risk areas. In several investigations on advanced computer-focused attacks, the Dutch NHTCU has collaborated with Russian authorities, CERTs and the private security industry to assist affected financial institutions worldwide and prevent further damage to the integrity of the financial system [640]. The No More Ransom Project united over 70 competitors in the private security sector, and public agencies from over 40 countries including Iran, Israel, Russia and Ukraine. In these collaborations, human security indeed prevails over national security.

Towards a fifth stage: technical harmonization Besides the incentive problem, an additional challenge in international collaboration is the technical processing of large cyber criminal data sets - think of the vast amount of data related to a takeover of a cryptomarket like Hansa - that are shared between networks of law-enforcement agencies. In other words, the investigative input of these networks - i.e., informational capitalism, read: the evidence about cyber criminals and cyber crimes - and their desired output (e.g., prosecution) might be obvious, but the processes between input and output are not. In reality, virtually all law-enforcement agencies only process the data they need to build a case (known as netto evidence), and are unable to fully index and access the total of collected data (known as bruto evidence), let alone that they have the means to normalize large raw data sets in unknown formats from other agencies, load those sets in their police systems, conduct advanced analyses on these sets, select suitable targets for investigations and overcome the incentive problem. The absence of uniform technical processes to process data increases the double whammy effect of deviant security, especially for less equipped agencies that share their operational data with third parties but are not able to process any received data. Scarce resources are wasted because of duplicate efforts of agencies and expensive commercial products to mine their data, and even lead to situations in which agencies are technically unable to use evidence for their investigations. The current situation also pushes towards the creation of a single connected ecosystem dominated by the few nodes that do have the resources to collect, process and analyze investigative data, often helped by closed-source technologies of a limited number of private security companies. Indeed, many of Ross Anderson's concerns about networks of government surveillance - information monopolies with network effects, low-marginal costs and technical lock-ins - are also real for the closed networks in which LEA operate, if only because law-enforcement and intelligence networks are increasingly intertwined [641].

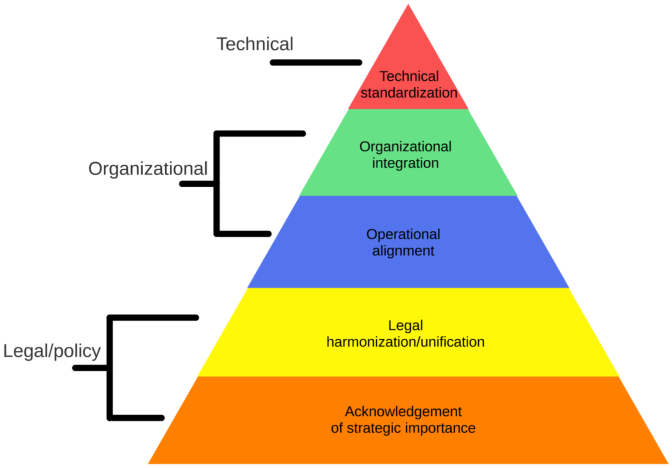

Technical
Technical standardization
Organizational
Organizational integration
Operational alignment
Legal/policy
Legal harmonization/unification
Acknowledgement of strategic importance

Figure 8.3: These five stages represent the different steps in international collaboration between law-enforcement agencies. Acknowledgement of strategic importance and legal harmonization/unification occur on a legal/policy level, operational alignment and organizational integration occur on an organizational level of harmonization while technical standardization is an outcome of technical harmonization. The model is now in use by the Dutch NHTCU to plot with which international public agencies the unit wants to increase, decrease, explore or consolidate investigative collaborations, i.e., the kind and degree of harmonization. The NHTCU might try, as an hypothetical example, to go from a situation of legal harmonization with another unit in which both units merely execute each other's MLATs, to a situation in which both units align operations, thus first explore and then increase collaborations.

One of the capstones against the above mentioned threats to human security and the double whammy effect of deviant security might well be *technical harmonization* between law-enforcement agencies of liberal democracies governed by the rule of law. Technical harmonization is about establishing universal ethical and technically uniform norms, criteria, methods and principles to process operational data by law-enforcement agencies. The term harmonization is purposely used. Harmonization between law-enforcement agencies implies alignment, fine-tuning and collaboration while preserving diversity. The term further relates to a degree of agility and flexibility which is needed for agencies in a dynamic world with rapidly changing technologies and (geo)politics whilst harmonization might also lead to more rigid standardization when needed [623][642, pp.91-92][643, p.52]. A practical implementation of this approach is that it promotes public consortia to develop databases, software and analytical models for law-enforcement agencies as much as possible, and subsequently share these technologies with like-minded public partners. This decentralized approach opens an opportunity to reduce the above outlined double whammy effect of deviant security and digital divide between law-enforcement agencies as investigative resources are more equally and fairly distributed among public partners. Indeed, only a single well-equipped public partner has to develop the technologies to normalize and/or analyze operational data.

Mandated breachers should develop their own technologies to process their evidence and avoid core technologies of commercial parties because this approach promotes human security and avoids the commodification of security. A first argument is to prevent a vendor lock-in. Investigations on cyber crime need a flexible range of tools to process ever-changing data sets without being dependent on the services of a private monopolist or having substantial switching costs. The second argument is far more important: power depends upon who owns code [607, p.534]. Any code used in investigations to process evidence must be transparent to legal practitioners, including the judiciary and defendants. Therefore, universities and other non-profit and non-governmental organizations are ideal partners to normalize data and subsequently exploit vulnerabilities of cyber criminals by developing advanced analytical models. Simultaneously, they can formulate and implement human-centric information ethics that provide human security, while helping to avoid securitization through bureaucratic processes and routines of legal practitioners [644, pp.125-127]. To conclude, technical harmonization is solely about processing data in a uniform and bottom-up manner between law-enforcement agencies, and not about binding rules or obligations mandating the sharing of any collected data. Sovereign democratic states governed by the rule of law are and ought to be in control of their own data, and subsequently have the legal, organizational and technical means to decide in which situations they want to share what data with which party. This might mean that independent oversight mechanisms such as the judiciary are not only needed in situations where data is shared, but also for the technologies that subsequently process data for investigative purposes.

8.4 Reactive & Proactive Investigations on Commission & Protection

The last research question of this study is: which profit-driven computer-focused suspects should be targeted by cyber crime units of national and federal law-enforcement agencies? There is a distinctive pattern found in investigations on profit-driven computer-focused crimes. This pattern is more in line with the idea of deliberate (read: targeted, by choice) and opportunistic (read: untargeted, by chance) resource-limited attackers [382, pp.24-25][645], than the idea of the 'all powerful attacker' that generates attacks for whichever vulnerability exists [646]. In general, advanced law-enforcement cyber crime units that operate on an international level conduct reactive public-private investigations on commission providers and autarkic cyber criminal organizations, while launching proactive public-public investigations on protection providers.

Autarkic/autonomous organizations and commission & protection providers
Advanced cyber crime units of federal/national law-enforcement agencies gen-

erally focus on three particular organized groups that commit profit-driven computer-focused crimes with an international impact. The first group consists of:

1. *Autarkic/autonomous cyber criminal organizations.* These closed groups have the assets to execute large parts of their MO themselves and make decisions autonomously. They may, for example, develop and operate their own malware, and subsequently launch deliberate APT-style attacks [647, p.9], like the Cobalt group that directly targeted financial institutions and took active measures to ensure that their malicious programs remained unknown to the cyber criminal and cyber security community alike [496]. Such a private group may have distinctive roles including their own in-house system administrator who sets up their bulletproof technical infrastructure, e.g., C&C, chat and VPN servers. Although they do not sell their home-grown valuables to (less-skilled) clients, and avoid relying on outsiders and outsourcing to the CaaS economy [251, p.3], they still might need others for e.g., post-activities such as money laundering. These organized groups are directly responsible for making high-value victims in - amongst others - the financial sector and as such affect the integrity of the global financial system. This is both a blessing and curse for them. The downside of generating high profits is that their malafide activities become noticeable to a very competitive cyber criminal community that is keen to identify the latest threats in cyberspace and share their findings with a broad audience, including law-enforcement agencies. Yet some of these private groups have shown that they have the assets to postpone their operations for a period of time when under attack by threat agents, only to reappear in a more robust - read: more secure - manner. In other words, they have the ability to work on projects instead of processes, and thus avoid recency and consistency as a vulnerability. They can also opt for a more security-driven approach in which confidentiality (via e.g., a closed-circuit MO and distrust of outsiders) and affecting integrity (through e.g., deception) is more important than availability (CI>A). (Investigations on) autonomous cyber criminal organizations include the groups behind exclusive banking malware that is not for sale in the underground economy as Buhtrap, Carbanak, Cobalt, Dyre, GCMan, Lurk and Metel [648][260][649][496]; and the Lazarus/Bluenoroff group(s) behind the SWIFT attacks [580].

Less autarkic groups and autonomous individuals, i.e., opportunistic attackers, may outsource large parts of their MO to criminal facilitators because they have too few intangible assets - human, information and/or organization capital - to set up their whole business process and security system themselves. Figure 6.2 shows the many products and services in the CaaS economy that support the commission of crime and protection of crime and the criminal. These facilitators enable large volumes of less-advanced, opportunistic cyber criminals to safely commit untargeted crime, and for this reason these providers come in sight of the cyber security community. Especially very successful providers have their own particular weaknesses. They are too centralized in the underground economy, offer (partly) automated services/products, have client databases and 24/7 support, and are generally not very transparent about their security to their customers. In other words, providers work in processes and have a more business-driven approach in which availability and integrity of their product/service is more important than confidentiality (AI>C). So the next classifications consist of two types of organized service and product providers within the CaaS economy:

2. *Providers of the commission of cyber crime.* Investigations on these providers include botnets-as-a-service like Mirai Botnet #14 [650], Cutwail [651], GameOver Zeus [416], and Simda [652]; exploit kits like Angler (related to the autonomous Lurk group [653]) and Blackhole [435]; banking trojans, e.g., Gozi [654]; hacking-as-a-service providers [655]; or ransomware-as-a-service such as Philadelphia [432], RaaSberry, Satan and Wildfire [656][657].

3. *Providers of the protection of crime and the criminal.* Investigations on these providers include bulletproof telecom providers like Ennetcom and PGP Safe [658][659]; secure markets like Alphabay, Darkode and Hansa [526][660]; bulletproof hosters like Virus/Powerhost and Maxided [661][662]; the CAV targeted in Europol's operation Neuland [663]; criminal spy shops as PSS Spyshop [664]; cryptocurrency launderers like a British citizen operating from Amsterdam, the Netherlands [665]; or reshipping services like the one mentioned in this academic paper [212].

The next paragraph shows that there are two distinguished approaches in investigating these three organized groups.

Avalanche as a hybrid commission and protection provider: a one-off exception today, but a common practice in the future?

The observed client panels of commission providers in this study generally only allow alterations related to making victims as compared to options to customize the usually pre-baked security features. The panel of ransomware-as-a-service Philadelphia, for example, only has functionalities as querying victim passwords, geographically locating victims, checking financial transactions, or changing the amount of the demanded ransom [432]. So, while we have seen several providers that offer multiple related services and/or products that either promote commission *or* protection - i.e., BPHs that also sell domain registration and DDoS protection - and collaborations between protection and commission providers like ransomware developers and crypters [666], Avalanche was the first major CaaS provider in the underground economy that offered a single integrated good with multiple components related to both commission *and* protection. The Avalanche hosting infrastructure was taken down by a consortium of academic, law-enforcement, private (security) and other public organizations in 2016. 800.000 domains were seized, sinkholed or blocked, and five individuals were arrested. Amongst other things, Avalanche functioned as a fast flux network for malware families like Qakbot, Rovnix and TeslaCrypt, and as a bulletproof infrastructure for Citadel, Marcher and Tinba [667]. In other words, the organized group behind Avalanche delivered a hosting infrastructure for the commission of financial malware and ransomware, and simultaneously double fast flux, bulletproof infrastructure and recruitment of money mules for the protection criminals and their crimes. Whether Avalanche remains a one-off exception of a hybrid commission and protection provider, or is a foretaste of what we can expect in the near future, remains the question.

Reactive public-private investigations on commission providers & autarkic cyber criminal organizations Interestingly, investigations on commission providers and autarkic collectives/autonomous groups have two commonalities. Firstly, operations are *reactively* initiated by law-enforcement agencies. Secondly, they are mostly conducted with substantial help of the *private security industry*. These two attributes are understandable. Autarkic cyber criminal organizations and the products/services of commission providers directly make victims, and are therefore vulnerable for detection by the private security industry. Because of the industry's bonafide security products and services for customers (read: potential and actual victims), private security researchers not only have a major financial incentive, but also a far better information position than LEA, to swiftly detect pre-activities and activities related to the commission of cyber crime. Compared to mandated breachers, most parties in the cyber security community are proactively identifying, collecting, sharing and analyzing the victim-related activities of commission providers and autarkic groups. Law-enforcement agencies understandably do not have that information position: they cannot install intrusion/detection systems on the networks of potential victims, nor do actual victims easily file a complaint when a breach is not made public. Because of this information asymmetry on victimization between the public and private sector, it is hard, if not impossible, for law-enforcement agencies to independently locate C&Cs servers or discover new malware. That is not to say that LEA and their investigations do not have added value within the border-centric view on cyber security and cyber crime. On the contrary, the information of the private security industry - such as malware samples, access logs on infected machines and IP-addresses referring to C&C servers - can provide input for hit/no-hit searches on existing data in police systems and for executing a range of offensive countermeasures such as information requests and the preservation of servers [228, p.69]. As depicted in Figure 8.4, the subsequent data syntheses and newly collected evidence can be used to link the observed *what* by the private sector to the observed *who* by law-enforcement agencies. This process of attributing criminal activities to suspects is indeed very much the core business of law-enforcement agencies for which they have the competencies, means and data.

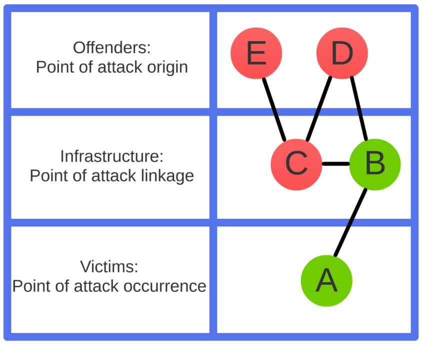


Figure 8.4: The private security industry generally has a better information position on the green circles as compared to the public cyber security community. Circle A may represent traces found on an infected machine of a victim such as malware. These traces may point to a C&C server as represented by circle B. LEA may preserve the server and request subscriber details. They now can match this evidence to data in their police systems or identify and preserve e.g., new servers or criminal communications like a mailbox (red circle C), and link that evidence to an online identity (red circle D). Red circle E may represent a DevSec provider who uses infrastructure C to communicate his/her product/service to client D. This client is now able to safely commit crime and make victims, while the DevSec provider stays largely out of sight to the private sector. Autarkic and autonomous criminal organizations execute large parts of an MO themselves, and are therefore represented by all circles from A to E.

Proactive public-public investigations on protection providers Investigations that successfully breach the security of protection providers hit the cyber criminal underground in the heart: the deviant security that ought to protect the cyber criminal and his/her crimes. DevSec services and products may fail in protecting their customers, and as a result many of these end-user criminals face little to no security at all. Suddenly, the unforeseen consequences of outsourcing their security to others are far greater than the original purpose of the countermeasure. Besides taking down their infrastructure and prosecuting the suspects involved, the reviewed investigations generated many new investigations on the clients of these services, read: end-user criminals with little or no capital to organize their own security. Moreover, while most commission providers on the CaaS market offer services/products that are specifically designed for computer-focused crimes, many of the DevSec providers offer services and products that can be used for the commission of computer-focused, assisted and enabled crimes as depicted in Figure 8.5. Thus, targeting successful DevSec brands with a good reputation, like bulletproof hoster Maxided, cryptomarket Hansa and bulletproof telecom provider Ennetcom [662][668][658], will not only have an impact on the cyber criminal underground, but potentially on computer-enabled crimes as well. The arguments of Section 3.3 suggest that investigations on DevSec providers are disruptive to the underground economy. Cyber criminals that are not arrested have to find a new DevSec provider, thus are forced to apply a suboptimal MO, with the associated risks of under protecting assets or over spending on deviant controls. When cryptomarkets Hansa and Alphabay were taken down, vendors and clients were forced to search for a new secure platform and moved to a legitimate chat service [669]. The encrypted communications might indeed help to protect identity but lacks a functioning reputation system as compared to cryptomarkets. As a result, ripping - read: harm to business assets - may increase.

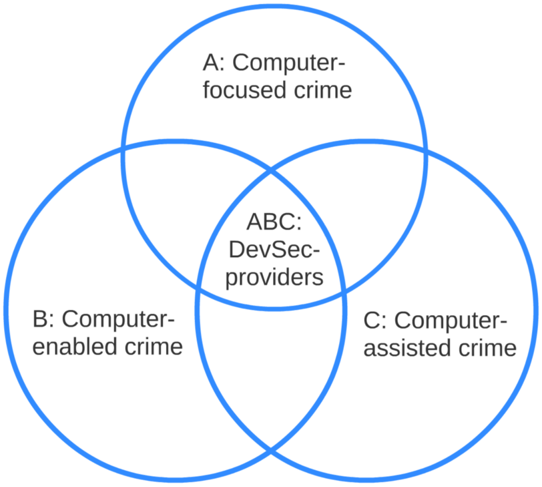

A: Computer-focused crime
ABC: DevSec-providers
B: Computer-enabled crime
C: Computer-assisted crime

Figure 8.5: From a good guy security perspective, DevSec providers (ABC) that offer fake IDs, bulletproof connections and hosting, encrypted telecommunications, preconfigured virtual machines and money laundering services are cross-cutting crime threat agents [599, pp.20, 56-57]. They not only protect those who commit *A: Computer-focused crimes* (e.g., ransomware operators), but also *B: Computer-enabled crimes* (e.g., online drug traders) and *C. Computer-assisted crimes* (e.g., identity fraudsters).

The reviewed investigations on DevSec providers have two common denominators. In general, they were *proactively* initiated by law-enforcement agencies. Secondly, the subsequent alliances were of a predominantly *public-public nature*, as compared to public-private collaborations. How can these two commonalities be explained? An unavoidable key problem for any successful CaaS provider is that they generate many data, and therefore become sooner or later noticeable to key players in the cyber security community. Generally, the private security industry and their clients - potential and actual victims - do *not* hold an information position on these DevSec providers in the preparation, pre-activity, activity and post-activity phase. Firstly, these commercial parties mostly focus on the *what* of end-user cyber criminals who are directly responsible for launching attacks and making victims. Secondly, they have difficulties to attribute a used C&C server or VPN connection to a specific bulletproof provider, let alone they can attribute a fake ID or preconfigured virtual machine to the responsible CaaS provider. As a consequence, LEA should not expect, and thus wait for, victims to file a complaint against a DevSec supplier or the private security industry to *en masse* provide intelligence reports about these providers.

In contrast, especially mandated breachers with offensive countermeasures have the ability to attribute DevSec products and services to specific providers. Because bulletproof connectivity and hosting providers sometimes mimic to be legitimate entities, they may use their real credentials to set up their financial, legal and technical infrastructure. If the credentials of a particular DevSec provider are significantly more often found compared to credentials of other facilitators than alarm bells might sound at a police office. Besides such statistical analyses, LEA have the qualitative research methods and techniques to identify DevSec providers. They can, for example, interrogate cyber criminals about fake ID providers or request subscriber information about bulletproof VPN servers at legitimate ISPs. Thus, law-enforcement agencies are the designated key player in the cyber security community to identify DevSec providers. As a consequence, they need a proactive attitude towards this particular group of cyber criminals, and launch investigations through their own analytical efforts. That is not to say that LEAs have to conduct investigations without outside help. A number of other public nonprofit bodies, including academia, CERTs and NGOs, have the competencies, means and data to target DevSec providers. No wonder that a consortium of - amongst others - bulletproof hosters launched major DDoS attacks in 2013 on the technical infrastructure of The Spamhaus Project - a nonprofit organization that collects and publishes data about BPH servers.

8.5 Interim Conclusion & Discussion

This purpose of this chapter is to present evidence-based approaches for appropriate investigative responses against deviant security practices of profit-driven computer-focused criminals with an international impact. Much of the normative frameworks are derived from security studies, while microeconomics helps to explain how investigations on transnational cyber crime work on a global level. Solely regarding the *ultimum remedium* of criminal law as the prime instrument against DevSec is a too narrow focus. Therefore, besides the recommendations for future work in the next paragraphs that will improve police investigations, researchers should also look at other tools of the regulatory tool-box of Internet governance to steer unwanted human behavior and affect deviant security practices [619]. Social norms, market mechanisms and architecture of technologies enforced by a range of cyber security key players other than LEA might have an impact as well [609]. These insights will hopefully lead to a truly multidisciplinary multi-stakeholder approach against the protection of cyber criminals.

On security-driven investigations that provide human security and Internet as a global public good This study sets out a normative framework for investigations on profit-driven computer-focused crimes. Basically, investigations in liberal democracies governed by the rule of law should become means to provide human security. This form of security predominantly focuses on the vulnerabilities of citizens, and related non-human and non-individual entities that affect citizens such as critical infrastructures. However, investigations that provide human security can be threatened by i) LEA and the private security industry when harming citizens, ii) offensive countermeasures of cyber criminals for deviant security purposes, and iii) other states for reasons of national security. Therefore, this study argues that LEA need to install a variety of administrative, physical and technical controls to make investigations security-driven. Further debate is needed with the cyber security community at large - including academics and legal practitioners - what human security in cyberspace encompasses and what not, and how to implement related human-centric information ethics in legitimate actions against cyber crime. For instance, the Dutch NHTCU and a private security company were criticized after taking over and subsequently using the Bredolab botnet to inform its victims in 2010 [670][671]. Yet there are as of today no efficient (read: scalable) and effective mechanisms to identify, notify and assist botnet victims to disinfect their systems. A further limitation of the proposed approach is its implementation of an inherently Dutch governmental policy view on cyberspace. Indeed, more comparative research is needed on investigative approaches of other liberal democracies. Yet investigation units of smaller states, like the Netherlands, are well equipped to make a diplomatic effort and promote the approach on a global level [611, pp.90-91]. The Dutch NHTCU, for example, is well represented in many international cyber security platforms and holds a strategic position in the larger cyber security network as Dutch servers are frequently misused as point of attack linkage.

On investigations as a public service with multiple outcomes Taking into account the normative framework of investigations as security-driven means that breach security to provide human security, this study argues that law-enforcement agencies should transform their investigations into a public service model within public-private alliances that have multiple outcomes. These investigations, in which the public interest prevails over private interests, evolve around two victim-based and two offender-based outcomes. The former are damage mitigation for potential victims and victim assistance to help actual victims. The latter outcomes are disruption of the cyber criminal process and attribution for prosecution purposes. While victim assistance and attribution have a firm legal basis, damage mitigation and disruption by mandated breachers have not, respectively e.g., sharing intelligence about suspects, like nicknames, with the larger cyber security community, or spreading disinformation about cyber criminals to undermine trust mechanisms. The power of cyber crime law is affected by its few possible outcomes, and primary focus on investigation, trial and sentence. Because convictions *in absentia* of suspects who are located in safe havens are inadequate, legislators need to discuss if disruption should become an alternative tool for LEA to confront cyber crime and turn the tide on the effectiveness crisis in investigations. Several academic scholars have already made similar arguments [92], while others proposed to disrupt, for example, cyber criminal fora [197, pp.169-170][672][269, p.5]. We therefore need to understand which interventions effectively disrupt MOs of successful cyber criminals and the cyber criminal underground at large, and research the legal feasibility of these methods. Although this study has reviewed few investigations on the computer-assisted crime of CSAM, a limitation of this chapter is that the investigative approach is not specifically made and tested for operations against sexually-driven online crimes. How can CSAM units exploit their data to the fullest and provide human security? Which stakeholder parties can contribute to these investigations? At the same time, investigations on profit-driven computer-focused crimes can learn from investigations on child sexual abusive material how to provide human security as the well-being of a child victim, irrespective of its nationality, gender or age, is of primary importance to legal practitioners of the latter type of investigation. Additionally, this study does not discuss online supervision of potential key enablers of cyber crime. Future studies should therefore focus on identifying high-risk individuals who are vulnerable to commit cyber crime, and what effective deterrence strategies would look like. Ultimately, new findings about supervision and investigations will help law-enforcement agencies to confront cyber crime in a more holistic manner.

On technical harmonization for a global investigation system This study further describes the current global investigation system on transnational cyber crimes, and provides evidence why this system does not work as deviant security practices take away incentives based on national interests to initiate an investigation. Before providing solutions to this incentive problem, this study first describes how international collaboration between law-enforcement agencies progresses through four stages, namely acknowledgement of strategic importance, legal harmonization, operational alignment and organizational integration. Besides overcoming geopolitical barriers and searching for common interests in human security over national security, a fifth phase in international collaborations - technical harmonization between law-enforcement agencies of liberal democracies governed by the rule of law - might be a first step to structurally fix the global investigations system. Smaller states as the Netherlands not only have a vested interest in channeling the discourse on the Internet's public core towards standardization [611, p.91], but also in investigations. Therefore, the Dutch NHTCU invested in technical harmonization by developing and subsequently sharing tools with other law-enforcement agencies. The next breakthrough for technical harmonization, however, will be the participation of other public stakeholders, such as but not limited to the academic world building software for law-enforcement agencies. While academics have acknowledged the need for standardization for research on cyber crime [345], too many investigative tools seem to be merely developed by academics as proof of concept and are not adopted by law-enforcement agencies. Scholars and legal practitioners both claim to serve the public interest. If this is true, than academics have a starting point to do multidisciplinary research with the police, and subsequently have the opportunity to have a lasting impact on how investigations in cyberspace are conducted by building software that does human security by design. Indeed, as Lawrence Lessig argues, code is law as software has the ability to determine the behavior of, in this case, law-enforcement agencies [607]. Moreover, besides having the same technical standards for data processing, equal investments are needed for international legal standardization for collecting, preserving and presenting digital evidence [619, p.358].

On reactive & proactive investigations on commission & protection
The last section of this chapter focuses on what the targets should be of security-driven investigations that provide human security. There is a distinctive pattern found in law-enforcement operations against profit-driven computer-focused crimes. Reactive public-private investigations focus on commission providers and autarkic/autonomous cyber criminal organizations. Proactive public-public investigations generally aim at protection providers. So investigations as public service with multiple outcomes will predominantly serve the first type of operations, while technical harmonization will also help public agencies to gain insights into the hidden world of DevSec providers. What is so far missing, however, are metrics to determine which successful providers and groups LEA should target to have the biggest impact on both the cyber criminal as well as cyber security communities, including potential and actual victims. Some services and products might be more important in the cyber criminal value chain than others, and identifying the choking points in their preparation, pre-activity, activity and post-activity phases are crucial. Moreover, are there displacement effects of clients migrating from successful, thus noticeable, CaaS enterprises to other, less known service/product providers that are not yet on the radar of the cyber security community, as suggested by experts [434]? In fact, in-depth research on specific commission and protection providers is still missing at large. While Europol names fake IDs as one of three 'cross-cutting crime threats with a significant impact across the spectrum of serious and organised crime' [599, pp.20, 56-57], no academic studies are found that describe the methods of working of this online CaaS provider, nor of e.g., suppliers of preconfigured VMs while their product poses a forensic challenge to investigators [673]. Moreover, governments should also find ways to increase the number of victim complaints of cyber crime. Victims do not only provide valuable evidence for reactive public-private investigations [635], but their official and unofficial complaints are foremost means to notify the state that their security has been breached by cyber criminals, and as such a request to restore human security and security as a collective public good. It is therefore of utmost important that all key players in the cyber security community notify the police, not only when they have become a victim, but also when they are a witness of cyber crime.

Part IV

Conclusions

Chapter 9

The Outlook of Deviant Security

Over the last years, there has been an ongoing debate about how cyber criminals are 'going dark', and how investigations are becoming less effective as a result. The security practices of cyber criminals are one of the underlying reasons of this problem. This research project takes predominantly profit-driven computer-focused criminals, and to a lesser extent sexually-driven computer-assisted criminals (read: child sexual abusive material users), as referent objects of security to subsequently describe their technical computer security practices, and explain the economics behind these practices in the Information Age. In exploring this research direction, the study offers the first structured and systematic, in-depth analysis what these deviant security practices encompass, having unprecedented access to, and using public and confidential data from, the cyber criminal and cyber security communities. This chapter reiterates the thesis objectives, fills in the deviant security process cycle, summarizes the normative/empirical and descriptive/explanatory findings, and presents directions for future research.

9.1 Thesis Objectives Reiterated

This section discusses how successful the thesis goal and objectives are achieved. As mentioned in Section 1.1, the overall goal of this study is to:

- Present a new security paradigm, i.e., a first picture on deviant security to an academic and legal practitioner audience.

The specific objectives in support of this overall goal are to:

- Describe and explain the technical computer security practices of cyber criminals; and

- Explore investigative responses against their protective practices.

This thesis introduces a new paradigm with cyber criminals as referent objects of security of which the findings are summarized in Sections 9.2 and 9.3. More specifically, a first picture on deviant security practices is presented that describes and explains in a structured and systematic manner the defensive and offensive administrative, physical and technical controls of predominantly financially-driven computer-focused criminals and their cyber-crime-as-a-service providers, and to a lesser extent of sexually-driven computer-assisted criminals (i.e., CSAM offenders).

The granularity of the research lies in the sum of its truly multidisciplinary data usage, methodology and outcomes. Firstly, this study is based on normative and empirical - i.e., qualitative and quantitative - data from public and confidential sources of the cyber criminal and cyber security communities. This variety of data sources allows triangulation, while categories on deviant security are matured to a point in which saturation is reached and further sampling is not needed. Secondly, social science methods and techniques from Grounded Theory are applied to study the computer science understanding of technical computer security with law-breaking referent objects. Concepts from predominantly microeconomic theory are subsequently used to explain these technical computer security findings. As such, this study has conceptual density and explanatory power from a microeconomic perspective, while there is plenty of room for other academic disciplines to contribute to the development of deviant security in the future (see Section 9.4). Lastly, research outcomes about deviant security practices and subsequent investigative practices are presented in this study as socio-technical practices in the Information Age that occur within respectively substantive and procedural legal frameworks.

Whether the model also has durability over time remains the question. Law-making processes are dynamic, and legislation is subjected to change. As a result, any alterations in law may affect the normative and empirical findings of this study. The same goes for the impact of new information technologies on deviant security practices. No instances are found in which cyber criminals applied artificial intelligence to protect themselves and their crimes, while mainstream usage of Internet of Things, IPv6 and quantum computing might potentially be game changers in the cat and mouse game between the cyber criminal and the cyber security communities [674][228][675][676]. With respect to the formulation of investigative responses against deviant security practices, this study identifies numerous weaknesses of cyber criminals and explains how LEA could exploit them without revealing current investigative techniques and as a result harm ongoing investigations. Rather than proposing new far-reaching investigative powers, the study presents suggestions for investigation approaches that aim at fixing many existing challenges in law-enforcement agencies while avoiding securitization and commodification of security. The practical utility of these suggestions are proven by the implementation of the approaches by the Central and Regional Criminal Investigations Divisions of the national police in the Netherlands, and have further been evangelized to the larger international law-enforcement community. Thus while the impact of this study on the academic world remains to be seen, the valorization of knowledge to a legal practitioner audience has so far been considerable. Although a first and partial process evaluation of the suggested approach in Section 8.2 has been conducted [415], full process and effect evaluations of the other suggested investigative approaches are still absent.

9.2 A Filled-In Deviant Security Process Cycle

Security is regarded in this study as an ongoing process cycle - a cat and mouse game - between the cyber criminal and cyber security communities. The interplay between law-breaking and law-abiding entities, and their offensive and defensive activities, mutually shapes each others security. A security process cycle that captures this interplay has been developed by academics and industry experts to understand and improve the security of law-abiding referent objects with law-breaking threat agents. But such a cycle has so far not been applied vice versa, with the goal to understand the security of law-breaking referent objects. This section first reiterates how the security cycle is used in the literature reviews of Part I, and then fills in the components of a deviant security cycle based on the methodological, normative and empirical findings of respectively Parts II and III of this study.

Security process cycles reiterated To understand the new security paradigm with cyber criminals as referent objects in need of security against attacks from threat agents like law-enforcement agencies, this study first adapted the security process cycle of the Common Criteria for Information Technology Security Evaluation and the result is depicted in Figure 9.1. The importance of explicitly naming the security recipient is promoted by adding referent object as a new and central component, while existing components - i.e., threat agents, threats & attacks, vulnerabilities, risks, assets and countermeasures - remain in place.

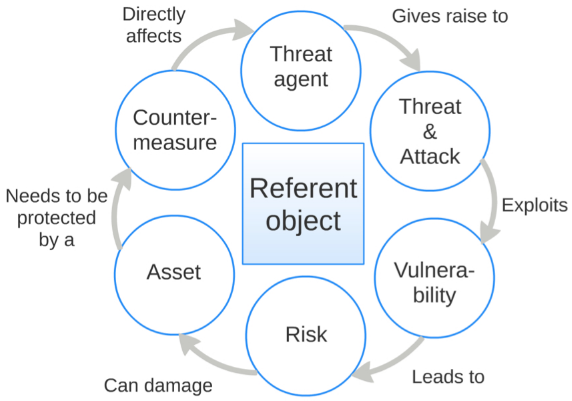


Figure 9.1: The relationship between various components of the security process. The cycle is based on the general model of the Common Criteria for Information Technology Security Evaluation [41, pp.40-43][59, p.27], and adapted by adding the components *referent object* and *attack*, and removing the component *exposure*.

The adapted cycle helps us i) to structure what the current good guy perspective is (i.e., with law-abiding entities as referent objects) on the computer science understanding of technical computer security, and the social science and legal/political understanding of cyber security and cyber crimes; ii) to structure what a bad guy perspective looks like with law-breaking referent objects (read: computer-focused and computer-assisted criminals) who apply technical computer security controls, and investigative responses from the cyber security and cyber crime discourses as depicted in Figure 9.2. The study then uses the security process cycle in a literature review on computer science, social science and legal research that touch upon the security controls of cyber criminals. The cycle shows that there are considerable gaps in our understanding how law-breaking referent objects protect themselves and their crimes. In other words, a full picture on deviant security practices is indeed - as stated in the introduction of this study - absent.

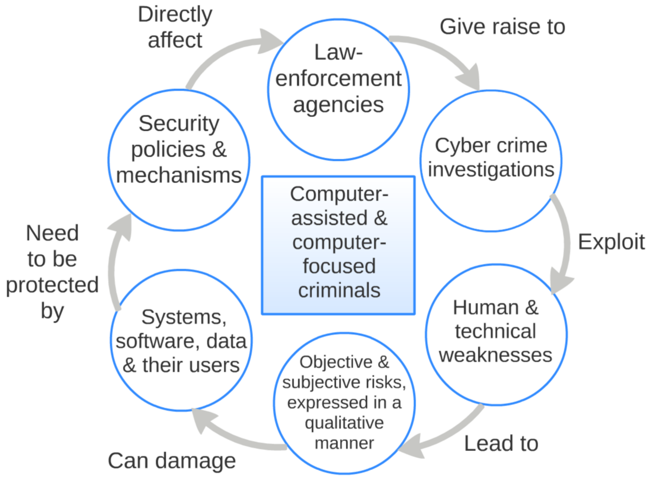

Directly affect
Law-enforcement agencies
Give raise to
Security policies & mechanisms
Cyber crime investigations
Computer-assisted & computer-focused criminals
Need to be protected by
Exploit
Systems, software, data & their users
Human & technical weaknesses
Objective & subjective risks, expressed in a qualitative manner
Can damage
Lead to

Figure 9.2: The components *Computer-assisted & computer-focused criminals*, *Law-enforcement agencies* and *Cyber crime investigations* are derived from the cyber security and cyber crime discourses. The components *Systems, software, data & their users* and *Security policies & mechanisms* are derived from the technical computer security discourse. The two components about weaknesses and risks are derived from both technical computer security and cyber security and cyber crime discourses.

Filling in a deviant security process cycle As depicted in Figure 9.3, the methodological, normative and empirical findings of Parts II and III enable us to fill in the security process cycle for cyber criminals in the Information Age. In short, referent objects of deviant security and their protective practices are defined and constructed by substantive and procedural law, yet shaped by cultural, macroeconomic, political and technological dimensions. Threat agents of cyber criminals - ranging from mandated breachers to criminal competitors - launch a range of attacks, while referent objects can also breach their own security on purpose or by accident. These attacks, accidents, failures and mistakes exploit a large variety of vulnerabilities in both the commission of crime as well as the protection of crime and the criminal. Absolute deviant security is impossible. There are always threat agents, while some vulnerabilities are even inherent to MOs, thus unavoidable. Other situations have iatrogenic effects, in other words, are vulnerability and countermeasure in one. These weaknesses lead to a number of risks that are expressed in this study in a qualitatively descriptive and explanatory manner, with subjective interpretations and beliefs of those who apply DevSec and those who are confronted by DevSec, and combined with objectively observable and/or measurable facts. Because of these risks, assets of the cyber criminal might be damaged. To secure their tangible and intangible valuables - including assets of a protective nature as deviant security is a scarce commodity and an asset to protect other assets - cyber criminals apply a range of offensive and defensive security policies and mechanisms in compensating layers. These deviant security practices directly affect the capabilities of threat agents, including law-enforcement agencies.

The cycle shows that deviant security and investigative responses are indeed a circular process, a cat and mouse game, with both sides constantly improving, innovating and implementing lessons learned, while having good reasons to hide their capabilities. This does not mean, however, that financially and/or sexually-driven cyber criminals control the game and gained the upper hand. There are too many external factors that negatively affect MOs, while profits - respectively money and sexual gratification - must be made. Ultimately, it is the sheer complexity of DevSec practices that is the enemy of law-breaking referent objects, but ironically, also of mandated threat agents when law-enforcement agencies do not understand the nature and extent of deviant security, and challenges and opportunities for their organizations. The next section zooms further in on the conclusions of the *how* and *why* of DevSec by giving i) a description of deviant security policies and mechanisms in the Information Age, and ii) an explanation of these practices using the economics of deviant security - i.e., microeconomics to understand the technical computer security practices of cyber criminals.

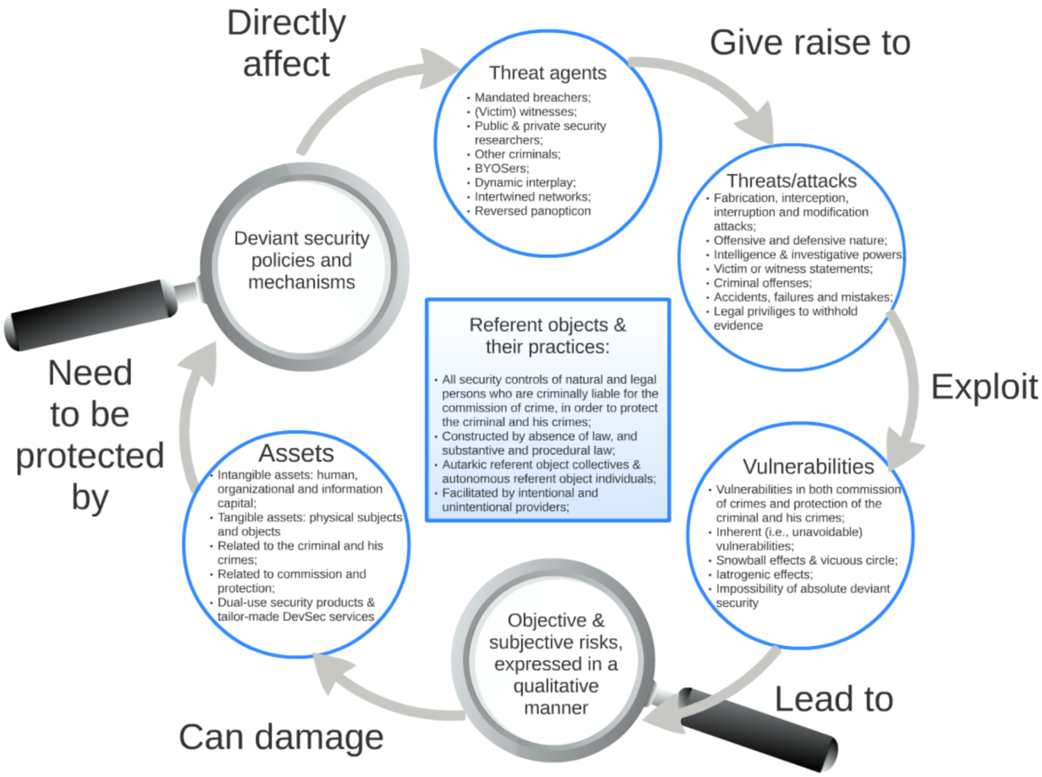

Directly affect
Threat agents
• Mandated breachers;
• (Victim) witnesses;
• Public & private security researchers;
• Other criminals;
• BYOSers;
• Dynamic interplay;
• Intertwined networks;
• Reversed panopticon
Give raise to
Threats/attacks
• Fabrication, interception, interruption and modification attacks;
• Offensive and defensive nature;
• Intelligence & investigative powers;
• Victim or witness statements;
• Criminal offenses;
• Accidents, failures and mistakes;
• Legal priviliges to withhold evidence
Exploit
Vulnerabilities
• Vulnerabilities in both commission of crimes and protection of the criminal and his crimes;
• Inherent (i.e., unavoidable) vulnerabilities;
• Snowball effects & vicuous circle;
• Iatrogenic effects;
• Impossibility of absolute deviant security
Lead to
Objective & subjective risks, expressed in a qualitative manner
Can damage
Assets
• Intangible assets: human, organizational and information capital;
• Tangible assets: physical subjects and objects
• Related to the criminal and his crimes;
• Related to commission and protection;
• Dual-use security products & tailor-made DevSec services
Need to be protected by
Deviant security policies and mechanisms
Referent objects & their practices:
• All security controls of natural and legal persons who are criminally liable for the commission of crime, in order to protect the criminal and his crimes;
• Constructed by absence of law, and substantive and procedural law;
• Autarkic referent object collectives & autonomous referent object individuals;
• Facilitated by intentional and unintentional providers;

Figure 9.3: The picture is a filled in version of the deviant security process cycle. Each component contains a selection of conclusions from this study. The two unspecified components with the magnifying glasses - deviant security policies and mechanisms, and the qualitative methodology and explanatory concepts of this essentially large-scale deviant security risk assessment - are discussed in more detail in the next Section 9.3.

9.3 Summary of Findings

While the previous section only briefly touches upon methodological, normative and empirical findings about (researching) the deviant security practices of cyber criminals, this section summarizes the descriptive and explanatory results based on the central research direction of this study: what are deviant security practices of cyber criminals?

A description of deviant security practices Grounded Theory was applied to describe the protective measures of cyber criminals. *How* cyber criminals protect crime and the criminal, and related vulnerabilities, are respectively described on the base of three research directions.

- The *what* researches the basic normative and empirical qualities of deviant security such as its:
  - ○ Legal definition and further construction by (absence of) substantive and procedural law, and empirically observable appearance and consequences;
  - ○ Meaning (i.e., state of being) as a subjective condition which is about the sense of cyber criminals about their own safety rather than an objective state which implies a situation of being without any threat;
  - ○ Provision as a club, common, private and public good, distributed in either a centralized or decentralized manner;
  - ○ Function as an asset to protect assets that relates to the criminal and his/her crimes; and
  - ○ Form as intangible and tangible, and as dual-use security product and/or tailor-made deviant security service.
- The *who* researches the interactive qualities of deviant security such as:
  - ○ Information asymmetries in intertwined networks;
  - ○ Deception tactics for the commission of crime with protective side effects, and deception tactics exclusively deployed for deviant security purposes. More specifically, a taxonomy that consists of masking, dazzling, decoying, mimicking, inventing, relabeling and double play;
  - ○ Trust as a three-step authentication process consisting of establishing cyber criminal identity (*who*), establishing (the outcomes of) criminal conduct (*what*) and enforcing trustworthiness through extra-legal governance; and
  - ○ Seven distrust controls, more precisely a taxonomy that consists of compartmentalization, data-minimization, regulations, investigations, labelling, testing and monitoring.
- The *when* and *where* researches the temporal-spatial qualities of deviant security such as:
  - ○ Controls against data volatility and retention like business continuity plans; using a single entity, a single time, for a single purpose; and secure-deletion and encryption of information capital;
  - ○ Intercultural communication in cyber crime in general and as a countermeasure specifically such as the use of monocultural communication and argot;

- Distribution as a countermeasure including the importance of a multipolar world, points of attack origin, linkage and occurrence, low and high-risk areas, location and time-boundedness and centralization, and extension, replacement, rotation and dispersion as distribution techniques; and
- Physical security of cyber criminals including the conversion of the online to the offline world, limited territorial control, micro external and internal security zones, physical protective objects (i.e., natural access control and technical surveillance) and subjects (e.g., violence by referent objects).

The defense and offense in-depth security layers of the Ponmocup botnet
Throughout this study, examples are given how the operators of the Ponmocup botnet protected themselves and their crimes. Reports on this botnet by the private security industry reveal that the sum of their security controls is truly defense and offense in-depth with multiple layers of security controls placed throughout their MO [391]. More precisely, the scheme had the following controls:

- Intangible and tangible (protective) products & services: having the human and organization capital to run a multi-million dollar profit operation for more than nine years, and rarely being noticed by the cyber security community, let alone experience arrests and/or takedowns;
- Information asymmetries in intertwined networks: actively collecting intelligence on the target's machine about potential law-enforcement activities;
- Deception as a countermeasure: dropping fake payloads on the machines of private security researchers;
- Trust and distrust mechanisms: trust - being active members of underground fora and collaborating with various affiliates and business partners; distrust - testing whether the malware runs on a private security researcher's machine, and the use of blacklists for e.g., usernames, computer names, services, drivers and product IDs;
- Countermeasures against data volatility and retention: deploying unique tokens, keys and encrypted binaries on a unique location per infected host;
- Intercultural communication as a countermeasure: using only a single national language - i.e., Russian - to communicate with affiliates and business partners;
- Distribution as a countermeasure: using separate servers for different functionalities, and avoiding attacks on victims located in former Soviet states.

Explanations for deviant security practices Based on the descriptive findings of this study, we conclude that referent objects of deviant security have to protect anything, against anybody, anywhere and at any time. How can we best explain these normative and empirical findings, and how should we regard these explanations? To begin with the last question, the sum of this study's findings about deviant security practices is a middle-range theory about the larger cyber criminal community that fits within the macro level paradigm of the Information Age. While deviant security practices can be explained by a range of micro level theories from several academic disciplines, the predominant focus of this study is on the economics of deviant security. This sub-discipline of the economics of information security and attacker economics first uses concepts from the computer science understanding of security to structure and explain the deviant security controls of cyber criminals. Microeconomic theory is then applied to subsequently explain the cost-benefit analyses of cyber criminals about their technical computer security controls. In practice, this means that the sum of the observed practices represents the full range of technical computer security controls, more specifically:

- Administrative, physical and technical countermeasures; of a
- Preventive, deterrent, detective, corrective, recovery and compensating nature; that provide the security goals of
- Confidentiality, availability and integrity; and related attributes of
- Accountability, anonymity, auditability, authenticity, non-repudiation, reliability, external and internal secrecy, undetectability, unobservability and unlinkability.

The observed deviant technical computer security practices are further explained by microeconomic concepts such as:

- Adverse selections, hidden actions and information, information asymmetries, distortions and monopolies, lemon markets, limited resource economies, moral hazards and (other) market failures;
- Coordination failures, customer data monetization, false accept and reject rates, free business model, negative externalities, negative and perverse incentives, and unproductive isolation;
- Taboo, tragic, value and zero-sum tradeoffs, and tradeoffs like deviation versus conformity, commission versus protection, autarky versus outsourcing, efficiency versus effectiveness, complexity versus accuracy, and secrecy versus transparency;
- Fixed, opportunity, total and variable costs, intangible and tangible costs, development and implementation costs, reputation and upfront costs, and ex-ante and ex-post controls, costs and losses;
- Competitive escalation, destructive, intercultural and value conflicts, excludability/rivalry, feedback loops, prisoner's dilemma, snowball effects, tragedy of the commons, vendor lock-ins, and vicious circles;
- Allocation problems, asset conversions, competitive disadvantages, illusion of control bias, objective and subjective value, optimism bias and return on investment;

Lastly, concepts from other disciplines are also used to explain deviant security practices like anthropology, linguistics, security studies and even medicine:

- Code switching, convergence, digital divide, dominant and third culture, iatrogenic effects, interlanguage, language acquisition, multilateral security, offensible spaces, political plausible deniability, security theater and word-sense disambiguation.

Ultimately, the overall result is a rich model on deviant security practices that has conceptual density, explanatory power and hopefully durability over time. The identified deviant security policies, mechanisms and related concepts do not stand on their own, but are interlinked, and should therefore be viewed in close coherence as shown in Figure 9.4. The nodes and edges in this figure further help to understand the complexity of the layers of security that cyber criminals receive and/or apply. Law-breaking referent objects have their own version of defense and offense security in-depth, aimed at and resulting in the protection of the criminal and his/her crimes against threat agents.

Investigative responses against deviant security practices Deviant countermeasures have a direct, negative impact on the responses of law-enforcement agencies. DevSec not only takes away the incentives to start an investigation, but also remains a burden for legal practitioners till the very end when a case is presented in court. Based on the findings of this study, investigative approaches against deviant security are developed, tested and now in use at the National High Tech Crime Unit and regional investigative cyber units of the Dutch national police. The normative framework of these approaches emphasizes the need for investigations to become security-driven means to provide human security and respect the Internet as a global public good. The practical implementation of this approach explains why investigations should be shaped as a public service with multiple stakeholders and outcomes that go beyond attribution. This study further sets out different stages for international collaboration and pleas for technical harmonization between law-enforcement agencies of liberal democracies. Lastly, evidence is given why proactive public-public investigations should target protection providers, while reactive public-private investigations should focus on autarkic/autonomous organized groups and commission providers.

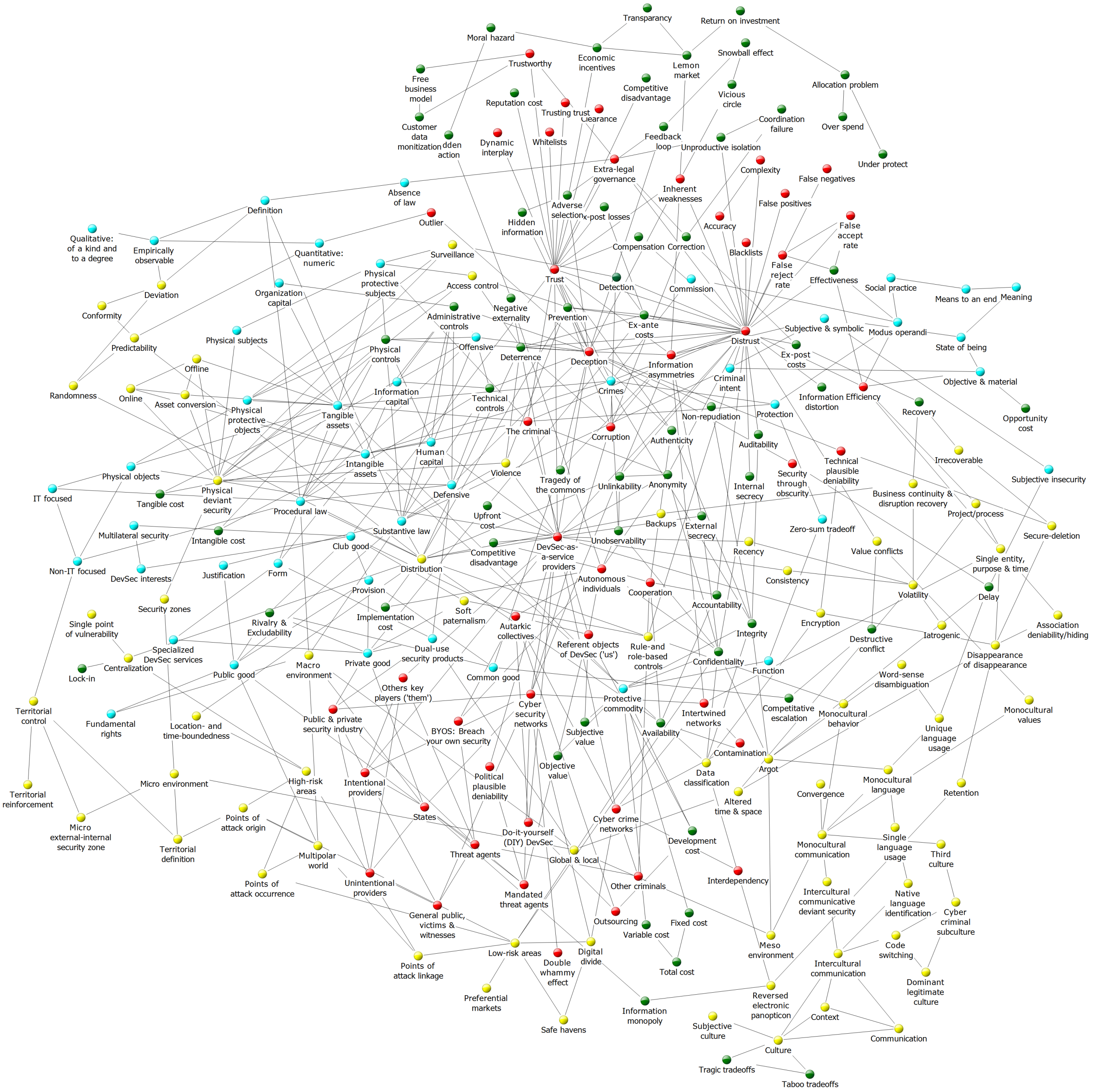


Figure 9.4: This network chart represents a selection of the key concepts of deviant security that are highlighted in *italic* throughout this study, and the interconnectedness of these concepts. Blue nodes depict the basic qualities of DevSec (what), red nodes the interactive qualities of DevSec (who), yellow nodes the temporal-spatial qualities of DevSec (when & where) and green nodes the explanatory concepts from predominantly the economics of deviant security (why). Although this chart highlights the vast complexity of DevSec, not all nodes and edges are added. More specifically, the detailed elaborations of specific controls have been left out such as the seven distrust controls, three steps of the trust process, and the specific techniques for access control and surveillance, as well as specific DevSec services/products and their providers, like bulletproof hosting, CAVs or online money laundering. Furthermore, only relations that have been mentioned in this study are drawn, while more links between concepts might be possible.

9.4 Moving Forward From Findings

Because the interim conclusion and discussion sections of the previous chapters give detailed recommendations for future work, this section focuses on the broad outlines and common threads of these sections on a high level of abstraction. What emerges from the recommendations of the interim conclusion and discussion sections is that deviant security has the potential to become an academic field of study on its own. There is a need for research of an interdisciplinary socio-technical-legal nature that combines the fields of law, science and technology studies. The common thread is that: i) there is plenty of room for other academic disciplines to study and explain deviant security, especially when a ii) mixed methods approach produces iii) outcomes that benefit legal practitioners.

New academic disciplines to study deviant security Section 3.1 reviews current computer science research that touched upon the security controls of cyber criminals. Indeed, there is still plenty of room for truly technical studies on deviant security, especially when such research projects explicitly take cyber criminals as referent objects. The computer engineering of deviant security, for example, could take a closer look at (malicious) software and hardware design used for protective purposes, including technical vulnerabilities and associated exploits. However, a big win for the new academic field of deviant security are a number of socio-technical disciplines on deviant security that combine social science with technical computer security. The psychology of deviant security, for example, may aim at understanding deviant security related behavior, thoughts and beliefs of cyber criminals. Cultural and social anthropology may focus on the security norms and values of specific cyber criminal communities, fora and autarkic/autonomous organizations, and related issues such as conflict resolution, taboo tradeoffs and learning processes of enculturation and socialization of the security culture of these collectives. Linguistics in general, and linguistic anthropology specifically, may further study in detail the role of technical computer security terminology, argot and national and ethnic languages as a security practice. Instead of narrowing down and zooming in, future work may also take a broader stand and go beyond security. The cyber criminals' *dependability* on computing and communication systems could be researched which includes attributes as maintainability, performance and safety [66]. Deviant security could also be placed within the grand sociological theory of the Risk Society [312][313][314]. From this perspective, more emphasis would be on risk as compared to (deviant) security, and the interplay of risk as a source of insecurity and related risk management for both cyber criminals and states. Such an approach would further research how the offensive capabilities of both key players create risks and uncertainties for both sides, and fuel each other's insecurity that in turn has to, but cannot fully, be governed.

A mixed methods approach to study deviant security Besides multiple disciplines to explain the security of cyber criminals, an interdisciplinary outlook may also mean applying a mixed methods approach as methodology. A first step might be to combine the qualitative findings of this project with more quantitative approaches to gain a more rich and in-depth multidisciplinary understanding of deviant security practices. Typologies on deviant security providers - such as bulletproof hosters and connectivity providers - can be used for automated role identification and property filtering. Grounded Theory research on deviant security benefits from using (un)supervised statistical research as topic modeling on cyber criminal writings to identify the security-related topics that cyber criminals discuss and as a guidance for new research directions in deviant security studies. Moreover, there is a need for the development of a monitor that quantifies the kind and degree of DevSec practices encountered by law-enforcement agencies in cyber crime investigations [218, p.11]. A monitor on DevSec will help investigative units to understand the security practices they face in a particular operation, and to make informed decisions how to exploit related vulnerabilities and which kind of legal practitioners are needed to successfully do so. The filled out monitors will produce statistics that show how DevSec standards change in time, and thus require the introduction or abolition of investigative powers. In this way, a DevSec monitor is a product of multidisciplinary scholarship on cyber crime that might contribute to evidence-based procedural law, comprehensive cyber security policies and effective investigations. Of course, these mixed methods work from two directions. Not only can qualitative findings be input for quantitative research, but quantitative descriptive findings can also be explained by qualitative research. There is also a world to win for quantitative descriptive research to identify patterns in deviants security practices that can subsequently be explained by qualitative research such as patterns in distribution as a countermeasure. The findings can be used to identify suspects, and formulate interventions aimed at exploiting especially unavoidable weaknesses like authorship analysis and native language identification. The results of this study also raise a more fundamental question about current statistical methods and techniques to measure the nature and extent of traditional and cyber crime. Because of a range of legitimate and illegitimate services and products that provide deviant security as a common, club, private and public good, less skilled offenders now have the means to effectively lower the visibility of themselves and their crimes. This democratization of deviant technical computer security will have an impact on the volume of unpunished crimes. While statistics suggest that visible traditional crime with direct victims is declining in jurisdictions like the Netherlands [677], cyber crime might equally be on the rise, yet far better protected, and as a result less measurable for academics that use traditional methods and techniques. Less than 30 possible instances of breaches via remote desktop protocol and no instances about providers of RDP were filed by the general public in the Netherlands in the years 2017 and 2018, although a private security researcher provided evidence how these suppliers made *en masse* victims in the Netherlands [678]. If so few data sources are available about direct victims of cyber crime, how effective are current data sources, methods and techniques - e.g., frequency counts of official complaints, self surveys - to gain a full picture on the nature and extent of those organized crimes that make *indirect* victims like bulletproof hosting and fake documents?

Outcomes that benefit legal practitioners The need for a mixed methods and multidisciplinary approach brings us to the output of academic research and its audience, or in other words, to the importance of connecting socio-technical findings about the security practices of cyber criminals to the normative world of legal practitioners. Throughout this study, examples are given about the combined social-technical-legal aspects of DevSec and investigative responses against deviant protective practices. New multidisciplinary research topics are diverse and plenty: from assessing the legal feasibility of investigative powers for disruptive purposes and the usage of statistical results of e.g., native language identification in court, to comparative legal studies on deviant security in substantive and procedural law; and from legal ethics in analytical models that exploit vulnerabilities and subsequently target suspects, to crime proofing of laws and policies that unnecessarily work as deviant security controls. As this is the first structured and systematic research project on deviant security, the long term outlook - particularly its impact on future research, law, policy and investigations - remains unknown, yet looks promising if we remember the lessons of the Dutch Parliamentary Inquiry Committee into Criminal Investigation Methods from 1994 to 1996. While reforming procedural law because of an integrity crisis within the Dutch national police, they warned legislators and the general public for the problem of traditional organized criminals who undisturbedly applied offensive physical countermeasures against legitimate government actions. Again, investigations are having a hard time but now face an effectiveness crisis because of technical computer security controls of criminals. Investigations are indeed what states make of it. Time and resources are needed to understand the protection of cyber crime and the cyber criminal, and subsequently increase the quality of the bureaucratic output of, and the public discussion about, the attribution process [19, p.33]. Many of the research outcomes of this project have been implemented by the Central and Regional Criminal Investigations Divisions of the Dutch national police, including recommendations to closely collaborate with academics to exploit the vulnerabilities in commission and protection. The research challenges are, however, multifaceted. On the one hand, we have to avoid that politicians, legislators and policy makers use DevSec for reasons of securitization and to demand ever-increasing investigative powers. On the other hand, both academics and legal practitioners have to collaborate far more intensively than they do now, and have to unlock the enormous potential of academic collaboration *with* the police instead of solely research *on* the police. The academic world needs the data and insights of law-enforcement agencies about cyber criminals and their crimes, while investigators need the power of independent thought. They might find each other in the understanding that more knowledge about deviant security serves the public interest. After all, deviant security is a *conditio sine qua non* of serious organized cyber and traditional crimes that undermine the very well-being of societies at large.

9.5 Concluding Remarks

This study introduced a new security paradigm: the technical computer security practices of (cyber) criminals. While there is academic, corporate, media and political attention for attacks by cyber criminals and defences and attacks by law-abiding entities, the security practices of cyber criminal referent objects were so far largely known unknowns. When these deviant security practices are discussed, the debate tends to evolve around encryption usage and anonymity. The journey of this study to literally and figuratively unravel all layers of deviant security lets us realize that we have to go beyond the current going dark debate as cyber criminals have many more deviant security controls at their disposal. If both academics and legal practitioners grasp the importance of understanding deviant security, than this is not a pessimistic outlook. On the contrary, the protection of crime and the criminal comes with all kinds of minor, major and even unavoidable vulnerabilities that the broader cyber security community should normatively and empirically explore to confront cyber crime more effectively. Studying deviant security is exciting as well. Not only because there are plenty of research opportunities to reveal what essentially does not want to be revealed, but also because of its significance: research outcomes have the ability to produce direct and tangible effects on the lives of citizens, especially the most vulnerable among us.

Bibliography

[1] D. E. Sanger and N. Perlroth, “Bank Hackers Steal Millions via Malware,” 2015. [Online]. Available: https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?mcubz=0

[2] ENISA, “National Cyber Security Strategies in the World,” 2013. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[3] NATO, “National Cyber Security Strategies,” 2014. [Online]. Available: https://ccdcoe.org/strategies-policies.html

[4] L. Hansen and H. Nissenbaum, “Digital disaster, Cyber security, and the Copenhagen school,” *International Studies Quarterly*, vol. 53, pp. 1155–1175, 2009.

[5] M. Dunn Cavelty, “Cyber-security,” in *Contemporary Security Studies*, A. Collins, Ed. Oxford University Press, 2012. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=2055122

[6] C. Osborne, “Carbanak hackers pivot plan of attack to target banks, the enterprise,” oct 2017. [Online]. Available: http://www.zdnet.com/article/carbanak-threat-group-change-plan-of-attack/

[7] Europol, “Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain,” mar 2018. [Online]. Available: https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

[8] C. Devereux, F. Wild, and E. Robinson, “The Biggest Digital Heist in History Isn’t Over Yet,” jun 2018. [Online]. Available: https://www.bloomberg.com/news/features/2018-06-25/the-biggest-digital-heist-in-history-isn-t-over-yet

[9] Tweede Kamer der Staten-Generaal, “Naar een effectieve en toekomstbestendige opsporing. Een eerste voortgangsnota Juni 2016 (bijlage

bij 29628,nr.643)," Vergaderjaar 2015-2016, 2016. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2016/06/20/tk-bijlage-3a-voortgangsnota-versterking-opsporing-juni-2016

[10] Ministerie van Veiligheid en Justitie, "Herijkingsnota. Herijking realisatie van de nationale politie," 2015.

[11] Tweede Kamer der Staten-Generaal, "Contouren voor een effectieve, toekomstbestendige opsporing (bijlage bij 29628,nr.593)," Vergaderjaar 2015-2016, 2015.

[12] N. Kop, "Van opsporing naar criminaliteitsbeheersing. Vijf strategische implicaties." Boom Lemma uitgevers, Den Haag, Tech. Rep., 2012.

[13] B.-J. Koops, "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research," in *Combatting Cybercrime and Cyberterrorism*, B. Akhgar and B. Brewster, Eds. Springer International Publishing, 2016, pp. 3–15. [Online]. Available: https://www.springerprofessional.de/en/megatrends-and-grand-challenges-of-cybercrime-and-cyberterrorism/10206532

[14] J. B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?" 2014. [Online]. Available: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[15] Europol, "iOCTA: Threat Assessment on Internet Facilitated Organised Crime," Europol, The Hague, Tech. Rep., 2011. [Online]. Available: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf

[16] A. Hess, "Encryption and Cyber Security for Mobile Electronic Communication Devices," apr 2015. [Online]. Available: https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices

[17] S. W. Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *The Journal of Criminal Law & Criminology*, vol. 97, no. 2, pp. 379–476, 2007.

[18] H. Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts," *Journal of International Affairs.*, vol. 70, no. 1, pp. 75–137, 2016. [Online]. Available: https://www.hoover.org/research/attribution-malicious-cyber-incidents-soup-nuts-0

[19] T. Rid and B. Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, jan 2015. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382

[20] I. Walden, *Computer Crimes and Digital Investigations.* Oxford University Press, 2007.

[21] S. W. Brenner, “Distributed Security: Moving Away from Reactive Law Enforcement,” *International Journal of Communications Law & Policy*, vol. 9, no. December, pp. 6–11, 2004. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=623283

[22] S. Ackerman, “FBI chief wants ’backdoor access’ to encrypted communications to fight Isis,” 2015. [Online]. Available: https://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis

[23] O. S. Kerr and B. Schneier, “Encryption Workarounds,” *SSRN Electronic Journal*, mar 2017. [Online]. Available: http://www.ssrn.com/abstract=2938033

[24] U. Gasser, N. Gertner, J. L. Goldsmith, S. Landau, J. S. Nye, D. O’Brien, M. G. Olsen, D. Renan, J. Sanchez, B. Schneider, L. Schwartzol, and J. L. Zittrain, “Don’t Panic: Making Progress on the ’Going Dark’ Debate,” Tech. Rep., 2016. [Online]. Available: https://dash.harvard.edu/handle/1/28552576

[25] P. Swire and K. Ahmad, “’Going Dark’ Versus a ’Golden Age for Surveillance’,” Center for Democracy and Technology, Tech. Rep., 2011. [Online]. Available: http://web.stanford.edu/{~}jmayer/law696/week8/GoingDarkorGoldenAge.pdf

[26] A. Keane, “Encryption substitutes,” 2017. [Online]. Available: https://www.hoover.org/research/encryption-substitutes

[27] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, “A comparison of security requirements engineering methods,” *Requirements Engineering*, vol. 15, no. 1, pp. 7–40, nov 2010. [Online]. Available: http://link.springer.com/10.1007/s00766-009-0092-x

[28] M. Yar, *Cybercrime and Society.* Sage Publications, 2006.

[29] Y. Jewkes, “Public policing and Internet Crime,” in *Handbook of Internet Crime*, Y. Jewkes and M. Yar, Eds. Cullompton: Willan, 2010.

[30] H. Nissenbaum, “Where Computer Security Meets National Security,” *Ethics and Information Technology*, vol. 7, no. 2, pp. 61–73, jun 2005. [Online]. Available: http://link.springer.com/10.1007/s10676-005-4582-3

[31] L. Zedner, *Security.* Routledge, 2009.

[32] A. M. Arnbak, “Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives,” PhD Thesis, Universiteit van Amsterdam, 2015. [Online]. Available: http://dare.uva.nl/record/1/492674

[33] B. Schneier, "iPhone Encryption and the Return of the Crypto Wars," 2014. [Online]. Available: https://www.schneier.com/blog/archives/2014/10/iphone{_}encrypti{_}1.html

[34] D. S. Wall, *Cybercrime: The transformation of crime in the information age.* Polity, 2007.

[35] A. Schmidt, "Secrecy versus openness: Internet security and the limits of open source and peer production," Ph.D. dissertation, Technische Universiteit Delft, nov 2014. [Online]. Available: http://repository.tudelft.nl/view/ir/uuid:ecf237ed-7131-4455-917f-11e55e03df0d/Am

[36] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley, 2008. [Online]. Available: http://www.cl.cam.ac.uk/{~}rja14/book.htmlhttp://portal.acm.org/citation.cfm?id=1373319

[37] J. de de Wilde, "Speaking or Doing Human Security?" in *The Viability of Human Security*, M. den Boer and J. de Wilde, Eds. Amsterdam: Amsterdam University Press, 2008, pp. 225–254.

[38] M. Junger, G. Laycock, P. Hartel, and J. Ratcliffe, "Crime science: editorial statement," *Crime Science*, vol. 1, no. 1, p. 1, 2012. [Online]. Available: http://www.crimesciencejournal.com/content/1/1/1

[39] E. G. Rød and N. B. Weidmann, "Empowering activists or autocrats? The Internet in authoritarian regimes," *Journal of Peace Research*, vol. 52, no. 3, pp. 338–351, may 2015. [Online]. Available: http://journals.sagepub.com/doi/10.1177/0022343314555782

[40] D. S. Wall, "The Devil Drives a Lada: The Social Construction of Hackers as Cybercriminals," in *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'*, C. Gregoriou, Ed. Palgrave Macmillan, 2012, pp. 4–18.

[41] Common Criteria, "Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5," Common Criteria, Tech. Rep. April, 2017. [Online]. Available: http://www.commoncriteria.org

[42] B. Goold and L. Zedner, "Introduction," in *Crime and Security*, B. Goold and L. Zedner, Eds. Hampshire: Ashgate, 2006, pp. xi–xxi.

[43] B. Buzan and L. Hansen, *The Evolution of International Security Studies.* Cambridge University Press, 2009.

[44] M. Castells, *The Information Age: Economy, Society, and Culture. Volume I: The Rise of the Network Society*, 2nd ed. Wiley-Blackwell, 2010.

[45] ——, *The Information Age: Economy, Society and Culture. Volume II: The Power of Identity*, 2nd ed. Wiley-Blackwell, 2010. [Online]. Available: http://doi.wiley.com/10.1002/9781444318234

[46] ——, "A Network Theory of Power," *International Journal of Communication*, vol. 5, pp. 773–787, 2011. [Online]. Available: http://ijoc.org/index.php/ijoc/article/view/1136/553

[47] J. P. Burgess, "Introduction," in *The Routledge Handbook of New Security Studies*, J. P. Burgess, Ed. Routledge, 2010, ch. 1, pp. 1–4.

[48] B. Buzan, O. Weaver, and J. de Wilde, *Security. A New Framework for Analysis.* London / Boulder, CO: Lynne Rienner Publishers, 1998.

[49] Motorola, "The User Role in Information Security. Building effective and efficient environments in the age of mobility and social networking." Tech. Rep., 2010. [Online]. Available: www.motorola.com/services/government

[50] B. Sandywell, "On the globalisation of crime: the Internet and new criminality," in *Handbook of Internet Crime*, Y. Jewkes and M. Yar, Eds. Willan Publishing, 2010, ch. 3, pp. 38–66.

[51] P. Dourish and K. Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human-Computer Interaction*, vol. 21, no. 3, pp. 319–342, 2006.

[52] D. Bigo, "The Möbius Ribbon of Internal and External Security(ies)," in *Identities, Borders, Orders Rethinking International Relations Theory*, M. Albert, D. Jacobson, and Y. Lapid, Eds. Minneapolis: University of Minnesota Press, 2001, ch. 4, pp. 91–116.

[53] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 4th ed. Cengage Learning, 2012.

[54] C. P. Pfleeger, *Security in Computing.* Prentice Hall, 2006.

[55] M. Dunn Cavelty, "Cyber-Security," in *The Routledge Handbook of New Security Studies*, J. P. Burgess, Ed. Routledge, 2010, ch. 3, pp. 154–162.

[56] R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, vol. 29, no. 3, pp. 408–433, 2006.

[57] P. Sommer and I. Brown, "Reducing Systemic Cybersecurity Risk," Tech. Rep. January, 2011.

[58] R. J. Deibert and R. Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology*, vol. 4, no. 1, pp. 15–32, mar 2010. [Online]. Available: http://doi.wiley.com/10.1111/j.1749-5687.2009.00088.x

[59] S. Harris, *All-in-one CISSP Exam Guide*, 6th ed. New York, NY: McGraw-Hill, 2012.

[60] M. Bishop, “What Is Computer Security?” *IEEE Security and Privacy*, vol. 1, no. 1, pp. 67–69, 2003.

[61] H. Venter and J. Eloff, “A taxonomy for information security technologies,” *Computers & Security*, vol. 22, no. 4, pp. 299–307, may 2003. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0167404803004061

[62] A. Schmidt, “Conceptualizing internet security governance,” in *Fourth GigaNet Annual Symposium Sharm-El-Sheikh, Egypt 14 November 2009*, 2009. [Online]. Available: http://netdefences.com/wp-content/uploads/Schmidt-2009-Conceptualizing-Internet-Security-Governance.pdf

[63] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 2003.

[64] J. Biskup, *Security in Computing Systems: Challenges, Approaches and Solutions.* Springer, 2009.

[65] C. E. Landwehr, “Computer security,” *International Journal of Information Security*, vol. 1, no. 1, pp. 3–13, 2001.

[66] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” Tech. Rep., 2004. [Online]. Available: https://dl.acm.org/citation.cfm?id=1026492

[67] A. S. Tanenbaum and M. van Steen, *Distributed Systems: principles and paradigms.* Upper Saddle River, NJ: Pearson Education, 2006.

[68] S. Harris, *CISSP all-in-one-exam guide*, 5th ed. New York, NY: McGraw-Hill, 2010.

[69] P. Sommer, *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers.*, 3rd ed., Swindon, 2012.

[70] M. E. Wetzstein, *Microeconomic theory: concepts and connections*, 2nd ed. Routledge, 2013.

[71] D. E. Bambauer, “Conundrum,” *Minnesota Law Review*, vol. 96, no. 584, pp. 584–674, 2011. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=1807076

[72] M. Carr, “Public-private partnerships in national cyber-security strategies,” *International Affairs*, vol. 92, no. 1, pp. 43–62, 2016. [Online]. Available: https://academic.oup.com/ia/article-lookup/doi/10.1111/1468-2346.12504

[73] S. W. Brenner and L. L. Clarke, “Distributed Security: Preventing Cybercrime,” *The John Marshall Journal of Information Technology & Privacy Law*, vol. 23, pp. 659–710, 2005.

[74] A. Arnbak, “Any Colour You Like: The History (and Future?) of E.U. Network and Information Security Conceptualizations and Policy,” 2014.

[75] M. Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age.* Routledge, 2008.

[76] B.-J. Koops, “The Internet and its Opportunities for Cybercrime,” 2011. [Online]. Available: http://ssrn.com/abstract=1738223

[77] E. Muller, I. Helsloot, and R. van Wegberg, “Vormen van veiligheid,” in *Veiligheid en veiligheidszorg in Nederland*, 2nd ed., E. Muller, Ed. Kluwer juridisch, 2013.

[78] Y. Jewkes and M. Yar, “Introduction: the Internet, cybercrime and the challenges of the twenty-first century,” in *Handbook of Internet Crime*, Y. Jewkes and M. Yar, Eds. Cullompton: Willan Publishing, 2010, ch. 1, pp. 1–8.

[79] D. Wall, “Cybercrimes and the Internet,” in *Crime and the Internet: Cybercrimes and Cyberfears*, D. Wall, Ed. London: Routledge, 2001, ch. 1.

[80] D. S. Wall, “The Internet as a Conduit for Criminal Activity,” in *Information Technology and the Criminal Justice System*, A. Pattavina, Ed. Thousand Oaks, CA: Sage Publications, Inc., 2015, pp. 77–98.

[81] M. Lagazio, N. Sherif, and M. Cushman, “A multi-level approach to understanding the impact of cyber crime on the financial sector,” *Computers & Security*, vol. 45, pp. 58–74, 2014.

[82] B.-J. Koops, “Cybercriminaliteit,” in *Recht en computer*, 6th ed., S. van der Hof, A. R. Lodder, and G. Zwenne, Eds. Deventer: Kluwer, 2014, ch. 9, pp. 213–241.

[83] I. Walden, “Crime and Security in Cyberspace,” *Cambridge Review of International Affairs*, vol. 18, no. 1, pp. 51–68, apr 2005. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/09557570500059563?journalCode=ccam20

[84] M. Yar, “Online Crime,” Oxford Research Encyclopedia of Criminology, Tech. Rep., 2016. [Online]. Available: http://criminology.oxfordre.com/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-112?print=pdf

[85] National Rapporteur on Trafficking in Human Beings, “Child pornography. First report of the Dutch National Rapporteur,” The Hague, Tech. Rep., 2011.

[86] R. Broadhurst and K. Jayawardena, “Online Social Networking and Pedophilia. An Experimental Research 'Sting',” in *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior*, K. Jaishankar, Ed. CRC Press, 2011, ch. 6, pp. 79–102.

[87] M. Button, C. Lewis, and J. Tapley, “Not a victimless crime: The impact of fraud on individual victims and their families,” *Security Journal*, vol. 27, no. 1, pp. 36–54, apr 2014. [Online]. Available: http://www.palgrave-journals.com/sj/journal/v27/n1/abs/sj201211a.html

[88] M. Domenie, E. Leukfeldt, J. Jansen, J. van Wilsem, and W. Stol, *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Den Haag: Boom Lemma uitgevers, 2013.

[89] E. U. Savona and M. Mignone, “The Fox and the Hunters: How IC Technologies Change the Crime Race,” *European Journal on Criminal Policy and Research*, vol. 10, no. 1, pp. 3–26, 2004.

[90] R. Deibert and R. Rohozinski, “Beyond Denial Introducing Next-Generation Information Access Controls,” in *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*, R. Deibert, J. Palfrey, R. Rohozinski, and J. Zittrain, Eds. The MIT Press, 2010, ch. 1, pp. 3–13.

[91] B. Dupont, “Security in the age of networks,” *Policing and Society*, vol. 14, no. 1, pp. 76–91, mar 2004. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/1043946042000181575

[92] N. K. Katyal, “Criminal law in cyberspace,” *University of Pennsylvania Law Review*, vol. 149, no. 4, pp. 1003–1114, 2001.

[93] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” *Computers & Security*, vol. 30, no. 8, pp. 719–731, nov 2011. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0167404811001040

[94] B. Schneier, “Security vs. Privacy,” 2008. [Online]. Available: https://www.schneier.com/blog/archives/2008/01/security{_}vs{_}pri.html

[95] B.-J. Koops, “The Shifting "Balance' Between Criminal Investigation and Privacy. A case study of communications interception law in the Netherlands,” *Information, Communication & Society*, vol. 6, no. January 2014, pp. 380–403, sep 2003. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/1369118032000155311

[96] M. Button, “Security,” *Global Crime*, vol. 11, no. 1, pp. 83–85, 2010.

[97] M. Dunn Cavelty, “Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities.” *Science and engineering ethics*, vol. 20, no. 3, pp. 701–15, sep 2014. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/24781874

[98] I. Loader and N. Walker, *Civilizing Security*. Cambridge University Press, 2007.

[99] M. Boer, “Technology-led Policing in the European Union: An Assessment,” *Cahiers Politiestudies*, vol. 3, no. 20, pp. pp.42–58, 2011.

[100] J. Eriksson, “Cyberplagues, IT, and Security: Threat Politics in the Information Age,” *Journal of Contingencies and Crisis Management*, vol. 9, no. 4, pp. 200–210, 2001. [Online]. Available: http://doi.wiley.com/10.1111/1468-5973.00171

[101] M. Schulze, “Clipper Meets Apple vs. FBI-A Comparison of the Cryptography Discourses from 1993 and 2016,” *Media and Communication*, vol. 5, no. 1, pp. 54–62, mar 2017. [Online]. Available: http://www.cogitatiopress.com/mediaandcommunication/article/view/805

[102] M. Levi and D. S. Wall, “Technologies, Security, and Privacy in the Post-9/11 European Information Society,” *Journal of Law and Society*, vol. 31, no. 2, pp. 194–220, 2004. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-6478.2004.00287.x/abstract

[103] L. Zedner, “Liquid security: Managing the market for crime control,” *Criminology and Criminal Justice*, vol. 6, no. 3, pp. 267–288, aug 2006. [Online]. Available: http://crj.sagepub.com/cgi/doi/10.1177/1748895806065530

[104] ——, “Security, the state, and the citizen: the changing architecture of crime control,” *New Criminal Law Review*, vol. 13, no. 2, pp. 379–403, 2010.

[105] C. Shearing and J. Wood, “Nodal Governance, Democracy, and the New 'Denizens',” *Journal of Law and Society*, vol. 30, no. 3, pp. 400–419, sep 2003. [Online]. Available: http://doi.wiley.com/10.1111/1467-6478.00263

[106] L. Zedner, “The concept of security: an agenda for comparative analysis,” *Legal Studies*, vol. 23, no. 1, pp. 153–175, 2003.

[107] R. Deibert and R. Rohozinski, “Liberation vs. Control: The Future of Cyberspace,” *Journal of Democracy*, vol. 21, no. 4, pp. 43–57, 2010. [Online]. Available: https://www.journalofdemocracy.org/article/liberation-vs-control-future-cyberspace

[108] M. Neocleous, “Against security,” in *Crime and Security*, B. Goold and L. Zedner, Eds., 2006, pp. 13–21.

[109] K. Vibhute and F. Aynalem, *Legal Research Methods. Teaching Material*, 2009. [Online]. Available: https://chilot.files.wordpress.com/2011/06/legal-research-methods.pdf

[110] G. J. van Hardeveld, C. Webber, and K. O'Hara, "Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets," *American Behavioral Scientist*, vol. 61, no. 11, pp. 1244–1266, oct 2017. [Online]. Available: http://journals.sagepub.com/doi/10.1177/0002764217734271

[111] ——, "Expert perspectives on the evolution of carders, cryptomarkets and operational security," in *10th ACM Conference on Web Science*, Amsterdam, the Netherlands, 2018, pp. 6–10. [Online]. Available: https://websci18.webscience.org/wp-content/uploads/2018/01/WebSci18{_}Events{_}PreProceedings-6-Evolution{_}Darknet.pdf

[112] S. Sundaresan, D. McCoy, S. Afroz, and V. Paxson, "Profiling underground merchants based on network behavior," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*. Toronto, Canada: IEEE, jun 2016, pp. 62–70. [Online]. Available: http://ieeexplore.ieee.org/document/7487943/

[113] P. A. C. Duijn and P. P. H. M. Klerks, "Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement," in *Networks and Network Analysis for Defence and Security*, ser. Lecture Notes in Social Networks, A. J. Masys, Ed. Cham: Springer International Publishing, 2014, pp. 121–159. [Online]. Available: http://link.springer.com/10.1007/978-3-319-04147-6

[114] P. A. C. Duijn, V. Kashirin, and P. M. A. Sloot, "The relative ineffectiveness of criminal network disruption," *Scientific reports*, vol. 4, p. 4238, jan 2014. [Online]. Available: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3937802{&}tool=pmcentrez{&}rendertype=abstract

[115] M. Baccara and H. Bar-Isaac, "How to organize crime," *The Review of Economic Studies*, vol. 75, no. 4, pp. 1039–1067, 2008.

[116] R. Lindelauf, P. Borm, and H. Hamers, "The influence of secrecy on the communication structure of covert networks," *Social Networks*, vol. 31, no. 2, pp. 126–137, may 2009. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0378873309000021

[117] G. McCormick and G. Owen, "Security and coordination in a clandestine organization," *Mathematical and Computer Modelling*, vol. 31, no. 6, pp. 175–192, mar 2000. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0895717700000509

[118] K. von Lampe and P. O. Johansen, “Organized Crime and Trust: On the conceptualization and empirical relevance of trust in the context of criminal networks,” *Global Crime*, vol. 6, no. 2, pp. 159–184, may 2004. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/17440570500096734

[119] J. Ayling, “Criminal organizations and resilience,” *International Journal of Law, Crime and Justice*, vol. 37, no. 4, pp. 182–196, dec 2009. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1756061609000330

[120] B. H. Erickson, “Secret Societies and Social Structure,” *Social Forces*, vol. 60, no. 1, pp. 188–210, 1981.

[121] C. Morselli, C. Giguère, and K. Petit, “The efficiency/security trade-off in criminal networks,” *Social Networks*, vol. 29, no. 1, pp. 143–153, jan 2007. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0378873306000268

[122] I. Baggili, A. BaAbdallah, D. Al-Safi, and A. Marrington, “Research Trends in Digital Forensic Science: An Empirical Analysis of Published Research,” in *Digital Forensics and Cyber Crime*, M. K. Rogers and K. C. Seigfried-Spellar, Eds. Springer Berlin Heidelberg, 2012, pp. 144–157. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39891-9{_}9

[123] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol. 8, no. 7, pp. 64–73, 2010. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1742287610000368

[124] M. A. Caloyannides, “Forensics Is So "Yesterday",” *IEEE Security & Privacy*, vol. 7, no. 2, pp. 18–25, 2009.

[125] G. C. Kessler, “Anti-Forensics and the Digital Investigator,” in *Proceedings of the 5th Australian Digital Forensics Conference*, Perth Western Australia, 2007. [Online]. Available: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1000{&}context=adf

[126] S. L. Garfinkel, “Anti-Forensics: Techniques, Detection and Countermeasures,” in *2nd International Conference on Information Warfare and Security*, 2007, pp. 77–84. [Online]. Available: http://simson.net/clips/academic/2007.ICIW.AntiForensics.pdf

[127] C. S. Peron and M. Legary, “Digital Anti-Forensics: Emerging trends in data transformation techniques,” in *Proceedings of 2005 E-Crime and Computer Evidence*, 2005. [Online]. Available: http://www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf

[128] H. Berghel, “Hiding data, forensics, and anti-forensics,” *Communications of the ACM*, vol. 50, no. 4, pp. 15–20, apr 2007. [Online]. Available: https://cacm.acm.org/magazines/2007/4/5676-hiding-data-forensics-and-anti-forensics/abstract

[129] A. Jain and G. S. Chhabra, “Anti-forensics techniques: An analytical review,” in *7th International Conference on Contemporary Computing*. Institute of Electrical and Electronics Engineers, 2014, pp. 412–418.

[130] K. Dahbur and B. Mohammad, “The anti-forensics challenge,” in *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications*. New York, NY: ACM Press, apr 2011, pp. 1–7. [Online]. Available: http://dl.acm.org/citation.cfm?id=1980822.1980836

[131] P. Zdzichowski, M. Sadlon, T. U. Vaisanen, A. B. Munoz, and K. Filipczak, “Anti-Forensic Study,” NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Tech. Rep., 2015. [Online]. Available: www.ccdcoe.org

[132] M. Gul and E. Kugu, “A survey on anti-forensics techniques,” in *2017 International Artificial Intelligence and Data Processing Symposium*. Malatya, Turkey: IEEE, sep 2017, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/8090341/

[133] R. Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem,” *Digital Investigation*, vol. 3, pp. 44–49, sep 2006. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1742287606000673

[134] K. Conlan, I. Baggili, and F. Breitinger, “Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy,” *Digital Investigation*, vol. 18, pp. S66–S75, 2016.

[135] M. K. Rogers, “Anti-Forensics: The Coming Wave in Digital Forensics,” in *7th Annual CERIAS Information Security Symposium*, West Lafayette, Indiana, 2006. [Online]. Available: http://www.cerias.purdue.edu/news{_}and{_}events/events/symposium/2006/materials/pdfs/antiforensics.pdf

[136] M. C. Stamm and K. J. R. Liu, “Anti-forensics of digital image compression,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1050–1065, sep 2011. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5720310

[137] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, “Countering JPEG anti-forensics,” in *2011 18th IEEE International Conference on Image Processing*. IEEE, sep 2011, pp. 1949–1952. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6115854

[138] H.-M. Sun, C.-Y. Weng, C.-F. Lee, and C.-H. Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1392–1403, aug 2011. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5963159

[139] Rb. Midden-Nederland, "ECLI:NL:RBMNE:2015:8845," 2015. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2015:8845

[140] S. Zander, G. Armitage, and P. Branch, "A Survey of Covert Channels and Countermeassures in Computer Network protocols," *IEEE Communications Surveys*, vol. 9, no. 3, pp. 44–57, 2007.

[141] J. Reardon, D. Basin, and S. Capkun, "SoK: Secure Data Deletion," in *IEEE Symposium on Security and Privacy.* IEEE, may 2013, pp. 301–315. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6547117

[142] G. Dardick, C. L. Roche, and M. Flanigan, "Blogs: Anti-forensics and Counter Anti-forensics," in *Proceedings of the 5th Australian Digital Forensics Conference*, Edith Cowan University, Perth Western Australia, 2007, pp. 199–203. [Online]. Available: http://ro.ecu.edu.au/adf/21

[143] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," *Digital Investigation*, vol. 2, no. 2, pp. 147–167, jun 2005. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1742287605000307

[144] Rb. Amsterdam, "ECLI:NL:RBAMS:2012:BX2325," 2012. [Online]. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2012:BX2325

[145] M. Brand, C. Valli, and A. Woodward, "Malware Forensics: Discovery of the Intent of Deception," *Journal of Digital Forensics, Security and Law*, vol. 5, no. 4, pp. 31–42, dec 2010. [Online]. Available: http://ojs.jdfsl.org/index.php/jdfsl/article/view/142

[146] R. J. Walls, B. N. Levine, and M. Liberatore, "Effective Digital Forensics Research is Investigator-Centric," in *Proceedings of the 6th USENIX conference on Hot topics in security.* San Francisco, CA: USENIX Association Berkeley, 2011, pp. 1–11.

[147] S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, "Going Bright: Wiretapping without Weakening Communications Infrastructure," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 62–72, jan 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6357177/

[148] M. Perklin, "Anti-Forensics and Anti-Anti-Forensics," in *DefCon*, 2012.

[149] A. Martin, N. Nuno, and G. D. Andrade, "Battling Botnets with Digital Rights in Mind," *European Journal for Law and Technology*, vol. 3, no. 2, pp. 2–4, 2012.

[150] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," in *ACM Conference on Computer and Communications Security*, Alexandria, VA, 2008, pp. 3–14.

[151] M. Riccardi, R. Di Pietro, M. Palanques, and J. A. Vila, "Titans' revenge: Detecting Zeus via its own flaws," *Computer Networks*, vol. 57, no. 2, pp. 422–435, feb 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612003556

[152] C. Czosseck, G. Klein, and F. Leder, "On the Arms Race Around Botnets - Setting Up and Taking Down Botnets," in *3rd International Conference on Cyber Conflict*, C. Czosseck, E. Tyugu, and T. Wingfield, Eds. Tallinn: CCD COE Publications, 2011, pp. 107–120. [Online]. Available: http://www.ccdcoe.org/publications/2011proceedings/OnTheArmsRaceAroundBotnetsSettingUpAndTakingDownBotnets-Czosseck-Klein-Leder.pdf

[153] P. Wang, S. Sparks, and C. C. Zou, "An Advanced Hybrid Peer-to-Peer Botnet," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 2, pp. 113–127, apr 2010. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4569852

[154] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, and A. Alazab, "Cybercrime: The case of obfuscated malware," in *Global Security, Safety and Sustainability & e-Democracy. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, C. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush, and A. Al-Nemrat, Eds., vol. 99. Berlin, Heidelberg: Springer, 2012, pp. 204–211. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-33448-1{_}28

[155] L. Watkins, C. Kawka, C. Corbett, and W. H. Robinson, "Fighting banking botnets by exploiting inherent command and control vulnerabilities," in *9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE).* Fajardo, PR: IEEE, oct 2014, pp. 93–100. [Online]. Available: http://ieeexplore.ieee.org/document/6999411/

[156] J. Zhang, R. Perdisci, W. Lee, U. Sarfraz, and X. Luo, "Detecting stealthy P2P botnets using statistical traffic fingerprints," in *Proceedings of the International Conference on Dependable Systems and Networks.* Hong Kong, China: IEEE, jun 2011, pp. 121–132. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5958212

[157] P. Wagenaar, "Detecting botnets using file system indicators," MSc dissertation, pp. 1–47, 2012.

[158] D. Andriesse, C. Rossow, and H. Bos, "Reliable Recon in Adversarial Peer-to-Peer Botnets," in *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*. New York, New York, USA: ACM Press, 2015, pp. 129–140. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2815675.2815682

[159] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. J. Dietrich, and H. Bos, "SoK: P2PWNED - Modeling and evaluating the resilience of peer-to-peer botnets," in *IEEE Symposium on Security and Privacy*, 2013, pp. 97–111.

[160] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your Botnet is My Botnet: Analysis of a Botnet Takeover," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 635–647.

[161] J. Caballero, P. Poosankam, C. Kreibich, and D. Song, "Dispatcher: Enabling Active Botnet Infiltration using Automatic Protocol Reverse-Engineering," in *Proceedings of the 16th ACM conference on Computer and communications security*. New York, USA: ACM Press, nov 2009. [Online]. Available: http://dl.acm.org/citation.cfm?id=1653662.1653737

[162] H. Asghari, M. J. G. van Eeten, and J. M. Bauer, "Economics of Fighting Botnets: Lessons from a Decade of Mitigation," *IEEE Security & Privacy*, vol. 13, no. 5, pp. 16–23, sep 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7310846/

[163] K. K. e Silva, "How industry can help us fight against botnets: notes on regulating private-sector intervention," *International Review of Law, Computers & Technology*, vol. 31, no. 1, pp. 105–130, jan 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1275274

[164] Y. Nadji, M. Antonakakis, R. Perdisci, D. Dagon, and W. Lee, "Beheading Hydras: Performing Effective Botnet Takedowns," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. New York, NY: ACM Press, 2013, pp. 121–132. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2508859.2516749

[165] Y. Fu, B. Husain, and R. R. Brooks, "Analysis of Botnet Counter-Counter-Measures," in *Proceedings of the 10th Annual Cyber and Information Security Research Conference*. Oak Ridge, TN: ACM Press, 2015, pp. 1–4. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2746266.2746275

[166] M. H. Jhaveri, O. Cetin, C. Gañán, T. Moore, and M. J. G. van Eeten, “Abuse Reporting and the Fight Against Cybercrime,” *ACM Computing Surveys*, vol. 49, no. 4, pp. 1–27, jan 2017. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3022634.3003147

[167] J. Kuhn, “The Dyre Wolf Campaign Stealing Millions and Hungry for More,” 2015. [Online]. Available: http://securityintelligence.com/dyre-wolf/{#}.VSTYWBezhpm

[168] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. M. Voelker, S. Savage, and K. Levchenko, “Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs,” in *21st USENIX Security Symposium*, Bellevue, WA, 2012, pp. 1–16. [Online]. Available: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/mccoy

[169] R. Zheng, Y. Qin, Z. Huang, and H. Chen, “Authorship Analysis in Cybercrime Investigation,” in *Intelligence and Security Informatics. ISI 2003. Lecture Notes in Computer Science*, H. Chen, R. Miranda, D. Zeng, C. Demchak, J. Schroeder, and T. Madhusudan, Eds., vol. 2665. Berlin, Heidelberg: Springer, 2003, pp. 59–73. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-44853-5{_}5

[170] S. Afroz, A. C. Islam, A. Stolerman, R. Greenstadt, and D. McCoy, “Doppelgänger Finder: Taking Stylometry to the Underground,” in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. San Jose, CA: IEEE, may 2014, pp. 212–226. [Online]. Available: http://ieeexplore.ieee.org/document/6956566/

[171] A. Rashid, A. Baron, P. Rayson, C. May-Chahal, P. Greenwood, and J. Walkerdine, “Who am I? Analyzing digital personas in cybercrime investigations,” *Computer*, vol. 46, no. 4, pp. 54–61, 2013.

[172] N. Rosenblum, X. Zhu, and B. P. Miller, “Who wrote this code? Identifying the authors of program binaries,” in *Proceedings of the 16th European conference on research in computer security*, V. Atluri and C. Diaz, Eds. Berlin, Heidelberg: Springer, sep 2011, pp. 172–189. [Online]. Available: http://dl.acm.org/citation.cfm?id=2041225.2041239

[173] S. Alrabaee, N. Saleem, S. Preda, L. Wang, and M. Debbabi, “OBA2: An Onion Approach to Binary code Authorship Attribution,” *Digital Investigation*, vol. 11, pp. S94–S103, may 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287614000176

[174] R. Layton and A. Azab, “Authorship Analysis of the Zeus Botnet Source Code,” in *Fifth Cybercrime and Trustworthy Computing Conference*. Auckland, New Zealand: IEEE, nov 2014, pp. 38–43. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=7087326

[175] R. Layton, P. Watters, and R. Dazeley, "Unsupervised authorship analysis of phishing webpages," in *International Symposium on Communications and Information Technologies (ISCIT)*. Gold Coast, QLD, Australia: IEEE, oct 2012, pp. 1104–1109. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6380857

[176] M. Brennan, S. Afroz, and R. Greenstadt, "Adversarial stylometry: Circumventing authorship recognition to preserve privacy and anonymity," *ACM Transactions on Information and System Security*, vol. 15, no. 3, pp. 1–22, nov 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2382448.2382450

[177] R. Broenink, "Finding Relations Between Botnet C&Cs for Forensic Purposes," MSc dissertation, may 2014. [Online]. Available: http://essay.utwente.nl/64998/1/Broenink{_}MA{_}EWI.pdf

[178] A. Calleja, J. Tapiador, and J. Caballero, "The MalSource Dataset: Quantifying Complexity and Code Reuse in Malware Development," *IEEE Transactions on Information Forensics and Security*, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8568018/

[179] E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol, "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists," *Crime, Law and Social Change*, vol. 67, no. 1, pp. 21–37, feb 2017. [Online]. Available: http://link.springer.com/10.1007/s10611-016-9662-2

[180] B. Danet and S. C. Herring, "Introduction: Welcome to the Multilingual Internet," in *The Multilingual Internet: Language, Culture, and Communication Online*, B. Danet and S. C. Herring, Eds. University Press Scholarship Online, 2007.

[181] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610–613, oct 2006. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/17068253

[182] R. Anderson, "Why Information Security is Hard - An Economic Perspective," in *Seventeenth Annual Computer Security Applications Conference*. New Orleans, LA: IEEE, 2001, pp. 358–365. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=991552

[183] M. J. G. van Eeten and J. M. Bauer, "Economics of Malware: Security Decisions, Incentives and Externalities," 2008. [Online]. Available: http://www.oecd.org/internet/ieconomy/40722462.pdf

[184] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko, "Botcoin: Monetizing Stolen Cycles," in *Network and Distributed System Security*, San Diego, CA, 2014. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.403.186

[185] P. Pearce, V. Dave, C. Grier, K. Levchenko, S. Guha, D. McCoy, V. Paxson, S. Savage, and G. M. Voelker, "Characterizing Large-Scale Click Fraud in ZeroAccess," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY: ACM Press, nov 2014, pp. 141–152. [Online]. Available: http://dl.acm.org/citation.cfm?id=2660267.2660369

[186] C. Herley and D. Florencio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," in *Economics Of Information, Security And Privacy*, T. Moore, D. Pym, and C. Ioannidis, Eds. Springer, 2009, pp. 33–53. [Online]. Available: http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf

[187] C. Herley, "Why do Nigerian Scammers Say They are from Nigeria?" in *Workshop on the Economics of Information Security*, 2012. [Online]. Available: http://research.microsoft.com/pubs/167719/whyfromnigeria.pdf

[188] C. Kanich, N. Weavery, D. McCoy, T. Halvorson, C. Kreibichy, K. Levchenko, V. Paxson, G. M. Voelker, and S. Savage, "Show me the money: characterizing spam-advertised revenue," in *Proceedings of the 20th USENIX conference on Security*. San Francisco, CA: USENIX Association, aug 2011, pp. 1–15. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028082

[189] J. Douglas, A. W. Burgess, A. G. Burgess, and R. K. Ressler, *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime*, 3rd ed. Wiley, 2013. [Online]. Available: https://www.wiley.com/en-us/Crime+Classification+Manual{%}3A+A+Standard+System+for+Investigating+and+Classifying+Violent+Crime{%}2C+3rd+Edition-p-9781118305058

[190] S. Tong, R. Bryant, and M. Horvath, *Understanding criminal investigation*. Wiley-Blackwell, 2009.

[191] B. E. Turvey, "Modus Operandi, Motive, and Technology," in *Digital Evidence and Computer Crime*, E. Casey, Ed. Elsevier, 2011, ch. 9, pp. 285–304.

[192] H. Whittle, C. Hamilton-Giachritsis, A. Beech, and G. Collings, "A review of online grooming: Characteristics and concerns," *Aggression and Violent Behavior*, vol. 18, no. 1, pp. 62–70, jan 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1359178912001097

[193] J. Davidson and P. Gottschalk, "Characteristics of the Internet for criminal child sexual abuse by online groomers," *Criminal Justice Studies*, vol. 24, no. 1, pp. 23–36, mar 2011. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/1478601X.2011.544188

[194] E. Quayle and M. Taylor, *Child pornography. An internet crime.* East Sussex: Brunner-Routledge., 2003.

[195] E. R. Leukfeldt, E. R. Kleemans, and W. P. Stol, "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks," *British Journal of Criminology*, vol. 57, no. 3, pp. 704–722, 2017. [Online]. Available: https://academic.oup.com/bjc/article-lookup/doi/10.1093/bjc/azw009

[196] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, "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*, pp. 1–14, nov 2016. [Online]. Available: http://link.springer.com/10.1007/s10610-016-9332-z

[197] T. J. Holt, "Exploring the social organisation and structure of stolen data markets," *Global Crime*, vol. 14, no. 2-3, pp. 155–174, 2013. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/17440572.2013.787925

[198] A. C. Spapens, "Macro networks, collectives, and business processes," *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 18, no. 2, pp. 185–215, 2010. [Online]. Available: https://pure.uvt.nl/portal/en/publications/macro-networks-collectives-and-business-processes(1e83d2a6-0c2c-4193-a608-9e8223fa9575).html

[199] L. Tompson and S. Chainey, "Profiling Illegal Waste Activity: Using Crime Scripts as a Data Collection and Analytical Strategy," *European Journal on Criminal Policy and Research*, vol. 17, no. 3, pp. 179–201, sep 2011. [Online]. Available: http://link.springer.com/10.1007/s10610-011-9146-y

[200] T. J. Holt and E. Lampke, "Exploring stolen data markets online: products and market forces," *Criminal Justice Studies*, vol. 23, no. 1, pp. 33–50, mar 2010. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/14786011003634415

[201] T. J. Holt, "Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures," *Deviant Behavior*, vol. 28, no. 2, pp. 171–198, 2007.

[202] J. Lusthaus, "Trust in the world of cybercrime," *Global Crime*, vol. 13, no. 2, pp. 71–94, may 2012. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/17440572.2012.674183

[203] R. Broadhurst and K.-K. R. Choo, "Cybercrime and on-line safety in cyberspace," in *Routledge International Handbook of Criminology*, C. Smith, S. Zhang, and R. Barberet, Eds. New York: Routledge, 2011, pp. 153–165.

[204] K. Jaishankar, "Establishing a Theory of Cyber Crimes," *International Journal of Cyber Criminology*, vol. 1, no. 2, pp. 7–9, 2007.

[205] K. C. Seigfried-Spellar, R. W. Lovely, and M. K. Rogers, "Self-Reported Internet Child Pornography Consumers: A Personality Assessment Using Bandura's Theory of Reciprocal Determinism," in *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior*, 1st ed., K. Jaishankar, Ed. Boca Raton: CRC Press, 2011, ch. 5, pp. 65–78.

[206] S. D. o. N. Y. Department of Justice, U.S. Attorney's Office, "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps," mar 2018. [Online]. Available: https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

[207] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," 2010. [Online]. Available: http://dud.inf.tu-dresden.de/Anon{_}Terminology.shtml

[208] B. Arief, M. A. B. Adzmi, and T. Gross, "Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1–Attackers," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 71–76, jan 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7031833

[209] G. R. Newman and R. V. Clarke, *Superhighway Robbery: Preventing E-Commerce Crime.* Willan Publishing, 2003.

[210] J. Simpson and E. Weiner, "Stealth," in *Oxford English Dictionary.* Oxford: Oxford University Press, 1989. [Online]. Available: https://en.oxforddictionaries.com/definition/stealth

[211] B. Krebs, *Spam Nation: The Inside Story of Organized Cybercrime - From Global Epidemic to Your Front Door.* Sourcebooks, 2015.

[212] S. Hao, K. Borgolte, N. Nikiforakis, G. Stringhini, M. Egele, M. Eubanks, B. Krebs, and G. Vigna, "Drops for Stuff: An Analysis of Reshipping Mule Scams," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.* New York, NY: ACM Press, 2015, pp. 1081–1092. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2810103.2813620

[213] G. C. Moreira Moura, "Internet bad neighborhoods," Ph.D. dissertation, University of Twente, 2013. [Online]. Available: http://doc.utwente.nl/84507/

[214] J. Lusthaus, "Electronic Ghosts," *Democracy*, no. 31, pp. 45–57, 2014. [Online]. Available: http://www.democracyjournal.org/31/electronic-ghosts.php?nomobile=1{&}page=3

[215] E. R. Leukfeldt, Ed., *Research agenda. The human factor in cybercrime and cybersecurity.* Eleven International Publishing, 2017. [Online]. Available: https://www.nscr.nl/onderzoeksagenda-the-human-factor-cybercrime-and-cybersecurity/{#}

[216] C. The Judicial Conference Advisory Committees on Appellate, Bankruptcy and C. Rules, "Proposed Amendments to the Federal Rules of Bankruptcy, Civil, and Criminal Procedure," 2014.

[217] Ministerie van Veiligheid en Justitie, "Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)," pp. 1–8, 2013. [Online]. Available: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit/memorie-van-toelichting-wetsvoorstel-voor-versterking-aanpak-computercriminaliteit.pdf

[218] K. Finklea, "Law Enforcement Using and Disclosing Technology Vulnerabilities," Library of Congress. Congressional Research Service, Tech. Rep., 2017. [Online]. Available: https://fas.org/sgp/crs/misc/R44827.pdf

[219] K. D. Mitnick and W. L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers.* New York: Wiley, 2005.

[220] ——, *The Art of Deception: Controlling the Human Element of Security.* New York: Wiley, 2002.

[221] J. Long, *No Tech Hacking. A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.* Elsevier Publishing, 2008.

[222] H. Dang, "The Origins of Social Engineering. From Odysseus' Trojan horse to phishing on the Internet: Deception just won't go away." *McAfee Security Journal*, no. Fall, pp. 4–8, 2008. [Online]. Available: http://www.wired.com/images{_}blogs/threatlevel/files/mcafee{_}security{_}journal{_}fall{_}2008.pdf

[223] J. Remmelink, *Inleiding tot de studie van het Nederlandse Strafrecht*, 15th ed. Arnhem: Gouda Quint, 1996.

[224] A. 't Hart, *Openbaar Ministerie en rechtshandhaving.* Arnhem: Gouda Quint, 1994.

[225] D. Maimon, M. Alper, B. Sobesto, and M. Cukier, "Restrictive deterrent effects of a warning banner in an attacked computer system," *Criminology*, vol. 52, no. 1, pp. 33–59, 2014. [Online]. Available: http://doi.wiley.com/10.1111/1745-9125.12028

[226] C. Guitton, "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence," *International Journal of Cyber Criminology*, vol. 6, no. 2, pp. 1030–1043, 2012.

[227] Infosecurity, "Infosecurity Europe 2014 > Europol: We Need to Disrupt Cybercrime," apr 2014. [Online]. Available: http://www.infosecurity-magazine.com/news/infosecurity-europe-2014-europol-we-need-to/

[228] C. S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," *International Journal of Cyber Criminology*, vol. 9, no. 1, pp. 55–119, 2015.

[229] Z. Zhao, M. Sankaran, G.-J. Ahn, T. J. Holt, Y. Jing, and H. Hu, "Mules, Seals, and Attacking Tools: Analyzing 12 Online Marketplaces," *IEEE Security & Privacy*, vol. 14, no. 3, pp. 32–43, may 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7478573/

[230] D. J. Herring, "Legal Scholarship, Humility, and the Scientific Method," 2006.

[231] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research.*, 7th ed. Chicago: AldineTransaction, 2012.

[232] J. J. Rachlinski, "Evidence-Based Law," *Cornell Law Review*, vol. 96, no. 4, pp. 901–924, 2011. [Online]. Available: http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=3208{&}context=clr

[233] L. Epstein and G. King, "The rules of inference," *University of Chicago Law Review*, vol. 69, no. 1, pp. 1–100, 2002. [Online]. Available: http://medcontent.metapress.com/index/A65RM03P4874243N.pdf

[234] T. S. Ulen, "The Unexpected Guest: Law and Economics, Law and Other Cognate Disciplines, and the Future of Legal Scholarship," *Chicago-Kent Law Review*, vol. 79, no. 2, pp. 403–429, 2004. [Online]. Available: https://scholarship.kentlaw.iit.edu/cklawreview/vol79/iss2/5/

[235] T. E. George, "An Empirical Study of Empirical Legal Scholarship: The Top Law Schools," *Indiana Law Journal*, vol. 81, no. 1, pp. 141–161, 2006.

[236] M. Heise, "The Past, Present, and Future of Empirical Legal Scholarship: Judicial Decision Making and the New Empiricism," *University of Illinois Law Review*, no. 4, pp. 819–850, 2002. [Online]. Available: http://scholarship.law.cornell.edu/facpub/733/

[237] H. Asghari, M. J. G. van Eeten, A. M. Arnbak, and N. A. N. M. van Eijk, "Security Economics in the HTTPS Value Chain," in *The Twelfth Workshop on the Economics of Information Security*, Washington, D.C., 2013, pp. 1–35. [Online]. Available: http://www.econinfosec.org/archive/weis2013/papers/AsghariWEIS2013.pdf

[238] Hof Den Haag, "ECLI:NL:GHDHA:2014:88, Gerechtshof Den Haag, 200.105.418-01," 2014. [Online]. Available: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2014:88

[239] J. W. Creswell, *Qualitative Inquiry & Research Design. Choosing Among Five Approaches.*, 2nd ed. Sage, 2007.

[240] J. Corbin and A. L. Strauss, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.*, 3rd ed. Newsbury Park, CA: Sage, 2007.

[241] L. Webley, "Qualitative Approaches to Empirical Legal Research," in *Oxford Handbook of Empirical Legal Research*, P. Cane and H. Kritzer, Eds. Oxford: Oxford University Press, 2010, ch. 38, pp. 1–21.

[242] L. Epstein and G. King, "Building an Infrastructure for Empirical Research in the Law," *Journal of Legal Education*, vol. 53, no. 3, pp. 311–320, 2003.

[243] K. Charmaz, *Constructing Grounded Theory. A Practical Guide through Qualitative Analysis.*, 1st ed. Sage, 2006.

[244] B. G. Glaser, *Basics of grounded theory analysis: Emergence vs. Forcing.* Mill Valley, CA: Sociology Press, 1992.

[245] C. Willig, *Introducing Qualitative Research in Psychology*, 3rd ed. McGraw-Hill, 2013.

[246] J. Corbin and A. L. Strauss, "Grounded Theory Research: Procedures, Canons and Evaluative Criteria," *Zeitschrift fur Soziologie*, vol. 19, no. 6, pp. 418–427, 1990.

[247] A. L. Strauss and J. Corbin, "Grounded theory methodology: An overview," in *Handbook of qualitative research*, N. K. Denzin and Y. S. Lincoln, Eds. Thousand Oaks, CA: Sage Publications, 1994, ch. 17, pp. 273–285.

[248] U. Flick, *An Introduction to Qualitative Research*, 4th ed. London: Sage Publications, 2009.

[249] E. R. Kleemans, "Organized crime research: challenging assumptions and informing policy." in *Applied Police Research: Challenges and Opportunities*, E. Cockbain and J. Knutsson, Eds. London / New York: Routledge, 2014, ch. 6, pp. 57–67.

[250] C. Bijleveld, *Methoden en Technieken van Onderzoek in de Criminologie.* Den Haag: Boom Lemma Uitgevers, 2009.

[251] A. Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission," *Crime, Law and Social Change*, vol. 62, no. 1, pp. 1–20, aug 2014. [Online]. Available: http://link.springer.com/10.1007/s10611-014-9520-z

[252] D. Turovsky, "Moscow's cyber-defense: How the Russian government plans to protect the country from the coming cyberwar," jul 2017. [Online]. Available: https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense

[253] T. Fox-Brewster, "Russian Cops Bust Key Members Of World's Busiest Cybercrime Gang," feb 2016. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminds/{#}51fa0f0b227f

[254] M. A. Livengood, "Underground Business Models: Crimeware-as-a-Service (CaaS)," Tech. Rep., 2011. [Online]. Available: http://www.rwsp.org/projects/139-crimeware-sas-sa-sservice.html

[255] A. K. Sood and R. J. Enbody, "Crimeware-as-a-service. A survey of commoditized crimeware in the underground market," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 28–38, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ijcip.2013.01.002

[256] A. A. Cárdenas, S. Radosavac, J. Grossklags, J. Chuang, and C. J. Hoofnagle, "An Economic Map of Cybercrime," 2009. [Online]. Available: http://papers.ssrn.com/abstract=1997795

[257] D. S. Wall and M. Williams, "Policing diversity in the digital age: Maintaining order in virtual communities," *Criminology and Criminal Justice*, vol. 7, no. 4, pp. 391–415, nov 2007. [Online]. Available: http://crj.sagepub.com/cgi/doi/10.1177/1748895807082064

[258] E. Monsma, V. Buskens, M. Soudijn, and P. Nieuwbeerta, "Partners in Cybercrime," in *Advances in Cyber Security: Technology, Operations, and Experiences*, D. F. Hsu and D. Marinucci, Eds. New York, NY: Fordham University Press, 2013, pp. 146–170. [Online]. Available: http://fordham.universitypressscholarship.com/view/10.5422/fordham/9780823244560.001.0001/upso-9780823244560-chapter-008

[259] Group-IB, "State and Trends of the Russian Digital Crime Market 2011," Group-IB, Moscow, Tech. Rep., 2012.

[260] R. Stoyanov, "The Hunt for Lurk. How we helped to catch one of the most dangerous gangs of financial cybercriminals," 2016. [Online]. Available: https://securelist.com/the-hunt-for-lurk/75944/

[261] Europol, "Cybercrime Dependencies Map," Tech. Rep. [Online]. Available: https://www.europol.europa.eu/publications-documents/cybercrime-dependencies-map

[262] D. S. Wall, “Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace,” *Police Practice and Research*, vol. 8, no. 2, pp. 183–205, 2007.

[263] W. Newton Suter, *Introduction to Educational Research. A Critical Thinking Approach*, 2nd ed. Sage, 2012.

[264] E. Kleemans, “Organized Crime, Transit Crime, and Racketeering,” *Crime and Justice*, vol. 35, no. 1, pp. 163–215, jan 2007. [Online]. Available: http://www.journals.uchicago.edu/doi/10.1086/501509

[265] E. Babbie, *The Practice of Social Research*, 10th ed. Belmont, CA: Thomson Wadsworth, 2004.

[266] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker, “An analysis of underground forums,” in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. New York, New York, USA: ACM Press, 2011. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2068816.2068824

[267] T. J. Holt, “Examining the Forces Shaping Cybercrime Markets Online,” *Social Science Computer Review*, vol. 31, no. 2, pp. 165–177, sep 2012. [Online]. Available: http://ssc.sagepub.com/cgi/doi/10.1177/0894439312452998

[268] J. Goode and K. Lumsden, “The McDonaldisation of police-academic partnerships: organisational and cultural barriers encountered in moving from research on police to research with police,” *Policing and Society*, pp. 1–15, feb 2016. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/10439463.2016.1147039

[269] T. J. Holt, “Identifying gaps in the research literature on illicit markets online,” *Global Crime*, vol. 18, no. 1, pp. 1–10, jan 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/17440572.2016.1235821

[270] Council of the European Union, “Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on the Netherlands,” Council of the European Union, Brussels, Tech. Rep., 2015. [Online]. Available: http://www.statewatch.org/news/2016/aug/eu-council-cybercrime-evaluation-netherlands-07587-15.pdf

[271] G. Odinot, M. A. Verhoeven, R. L. D. Pool, and C. J. de Poot, “Cyber-OC in the Netherlands,” in *Cyber-OC - Scope and manifestations in selected EU member states*, G. Kasper, B.-H. Karsten, G. Odinot, M. Verhoeven, Y. Werner, R. Pool, C. de Poot, and L. Korsell, Eds. Wiesbaden: Bundeskriminalamt Criminalistic Institute, 2016, ch. II, pp. 15–100.

[272] Europol, “World’s biggest marketplace selling internet paralysing DDoS attacks taken down,” apr 2018. [Online]. Available: https://www.europol.europa.eu/newsroom/news/world’s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down

[273] SC Staff, “SC Awards Europe 2017: And the winners of this year’s awards are...” jun 2017. [Online]. Available: https://www.scmagazineuk.com/sc-awards-europe-2017-and-the-winners-of-this-years-awards-are/article/666876/

[274] R. Cooter and T. S. Ulen, *An Introduction to Law and Economics*, 5th ed. Pearson, 2007. [Online]. Available: http://works.bepress.com/robert{_}cooter/56

[275] J. W. Creswell, *Research design. Qualitative, Quantitative, and mixed methods approaches*, 2nd ed. SAGE Publications, Inc., 2009.

[276] G. McGhee, G. R. Marland, and J. Atkinson, “Grounded theory research: literature reviewing and reflexivity.” *Journal of advanced nursing*, vol. 60, no. 3, pp. 334–42, nov 2007. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/17908129

[277] K. Charmaz, “Grounded Theory,” in *Rethinking Methods in Psychology*, J. Smith, R. Harre, and L. van Langenhove, Eds. London: Sage Publications, 1996, ch. 3, pp. 27–49.

[278] I. T. Coyne, “Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries?” *Journal of advanced nursing*, vol. 26, no. 3, pp. 623–630, sep 1997. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/9378886

[279] M. Miles and A. Huberman, *Qualitative data analysis: A sourcebook of new methods*, 2nd ed. Thousand Oaks, CA: Sage, 1994.

[280] P. Rogaway, “The Moral Character of Cryptographic Work,” 2015. [Online]. Available: http://eprint.iacr.org/

[281] O. S. Kerr, “The Problem of Perspective in Internet Law,” *Georgetown Law Journal*, vol. 91, pp. 357–405, 2003.

[282] B. Welten, Projectgroep Visie op de politiefunctie, and Raad van Hoofdcommissarissen, *Politie in ontwikkeling: visie op de politiefunctie.* Den Haag: NPI, 2005. [Online]. Available: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/36670.pdf

[283] M. Castells, *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*, 2nd ed. Wiley-Blackwell, 2010.

[284] R. M. Kramer, "Trust and distrust in organizations: emerging perspectives, enduring questions," *Annual Review of Psychology*, vol. 50, pp. 569–598, 1999. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/15012464

[285] R. Hardin, "The street-level epistemology of trust," *Politics & Society*, vol. 21, no. 4, pp. 505–529, 1993. [Online]. Available: http://journals.sagepub.com/doi/abs/10.1177/0032329293021004006?journalCode=pasa

[286] A. Mas-Colell, M. D. Whinston, and J. R. Green, *Microeconomic Theory*. Oxford University Press.

[287] E. Beauregard and B. Leclerc, "An Application of the Rational Choice Approach to the Offending Process of Sex Offenders: A Closer Look at the Decision-making," *Sexual Abuse: A Journal of Research and Treatment*, vol. 19, no. 2, pp. 115–133, jun 2007. [Online]. Available: http://sax.sagepub.com/cgi/doi/10.1177/107906320701900204

[288] P. Hartel, M. Junger, and R. Wieringa, "Cyber-crime Science = Crime Science + Information Security," Centre for Telematics and Information Technology, University of Twente, Tech. Rep., 2011. [Online]. Available: http://eprints.eemcs.utwente.nl/18500/03/0{_}19{_}CCS.pdf

[289] R. V. Clarke, "Technology , Criminology and Crime Science," *European Journal on Criminal Policy and Research*, vol. 10, no. 1, pp. 55–63, 2004.

[290] Z. Xu, Q. Hu, and C. Zhang, "Why computer talents become computer hackers," *Communications of the ACM*, vol. 56, no. 4, pp. 64–76, 2013. [Online]. Available: http://dl.acm.org/ft{_}gateway.cfm?id=2436272{&}type=html

[291] G. E. Higgins, "Rational Choice, Low Self-Control, Digital Piracy: An Examination of the Role of Value," in *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior*, 1st ed., K. Jaishankar, Ed. Boca Raton, FL: CRC Press, 2011, ch. 9, pp. 141–154. [Online]. Available: http://citation.allacademic.com/meta/p{_}mla{_}apa{_}research{_}citation/1/2/4/9/3/p124939{_}index.html

[292] M. Bachmann, "The Risk Propensity and Rationality of Computer Hackers," *International Journal of Cyber Criminology*, vol. 4, no. 1, pp. 643–656, 2010. [Online]. Available: http://www.cybercrimejournal.com/michaelbacchmaan2010ijcc.pdf

[293] W. van der Wagen and W. Pieters, "From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks," *British Journal of Criminology*, vol. 55, no. 3, pp. 578–595, may 2015. [Online]. Available: http://bjc.oxfordjournals.org/lookup/doi/10.1093/bjc/azv009

[294] J. Beebe, "Basic Concepts and Techniques of Rapid Appraisal," *Human organization*, vol. 54, no. 1, pp. 42–51, 1995.

[295] D. B. Cornish and R. V. Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending.* New Brunswick, NJ; London: Transaction Publishers, 2014.

[296] ——, "The rational choice perspective," in *Environmental Criminology and Crime Analysis*, 1st ed., R. Wortley and L. Mazerolle, Eds. Cullompton, United Kingdom: Willan Publishing, 2008, ch. 2, pp. 21–47.

[297] F. H. Easterbrook, "Criminal Procedure as a Market System," *The Journal of Legal Studies*, vol. 12, no. 2, pp. 289–332, 1983.

[298] R. A. Posner, "An Economic Theory of the Criminal Law," *Columbia Law Review*, vol. 85, no. 6, pp. 1193–1231, 1985. [Online]. Available: http://www.jstor.org/stable/1122392?seq=1{#}page{_}scan{_}tab{_}contents

[299] L. Epstein and J. Knight, "Building the Bridge from Both Sides of the River: Law and Society and Rational Choice," *Law & Society Review*, vol. 38, no. 2, pp. 207–212, 2004.

[300] M. B. Machado, "Between control and hacker activism: the political actions of Anonymous Brasil," *História, Ciências, Saúde-Manguinhos*, vol. 22, pp. 1531–1549, dec 2015. [Online]. Available: http://www.scielo.br/scielo.php?script=sci{_}arttext{&}pid=S0104-59702015001001531{&}lng=pt{&}tlng=pt

[301] T. J. Holt, O. Smirnova, Y. T. Chua, and H. Copes, "Examining the risk reduction strategies of actors in online criminal markets," *Global Crime*, vol. 16, no. 2, pp. 81–103, 2015. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/17440572.2015.1013211?journalCode=fglc20

[302] A. M. Arnbak, "Watch Your Mouth: Why Talking '(Cyber-)Security' Is Popular, Complex and Deeply Political," 2014. [Online]. Available: https://www.axelarnbak.nl/2014/02/14/watch-your-mouth-why-talking-cyber-security-is-popular-complex-and-deeply-political/{#}{_}ftnref7

[303] J. Mills, A. Bonner, and K. Francis, "The Development of Constructivist Grounded Theory," *International Journal of Qualitative Methods*, vol. 5, no. 1, pp. 25–35, 2006. [Online]. Available: http://journals.sagepub.com/doi/full/10.1177/160940690600500103

[304] F. Stalder, "The Network Paradigm: Social Formations in the Age of Information," *The Information Society*, vol. 14, no. 4, pp. 301–308, 1998. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/019722498128755

[305] S. Fuller, "Book Review: The Information Age: Economy, Society and Culture," *Science, Technology & Human Values*, vol. 24, no. 1, pp. 159–166, 1999. [Online]. Available: http://journals.sagepub.com/doi/10.1177/016224399902400108

[306] T. Thygesen Vendius, "Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene|," *EJPS*, vol. 3, no. 2, pp. 151–161, nov 2015. [Online]. Available: http://www.maklu-online.eu/nl/tijdschrift/ejps/volume-3/issue-2/europols-cybercrime-centre-ec3-its-agreements-thir/

[307] G. Christou, "The challenges of cybercrime governance in the European Union," *European Politics and Society*, pp. 1–21, jan 2018. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430722

[308] European Parliament, "Police cooperation: MEPs approve new powers for Europol to fight terrorism," may 2016. [Online]. Available: http://www.europarl.europa.eu/news/en/press-room/20160504IPR25747/police-cooperation-meps-approve-new-powers-for-europol-to-fight-terrorism

[309] J. Monar, "Eurojust and the European Public Prosecutor Perspective: From Cooperation to Integration in EU Criminal Justice?" *Perspectives on European Politics and Society*, vol. 14, no. 3, pp. 339–356, sep 2013. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/15705854.2013.817807

[310] European Council and Council of the European Union, "20 member states confirm the creation of an European Public Prosecutor's Office - Consilium," oct 2015. [Online]. Available: http://www.consilium.europa.eu/en/press/press-releases/2017/10/12/eppo-20-ms-confirms/

[311] N. Bingham, "Reviews: The information age: economy, society and culture. Volume 1. The rise of the network society." *Environment and Planning B: Planning and Design*, vol. 25, no. 4, pp. 631–632, 1998. [Online]. Available: http://journals.sagepub.com/doi/abs/10.1068/b250631

[312] U. Beck, *Risk Society: Towards A New Modernity.* London: Sage Publications, 1992.

[313] D. Garland, *The Culture of Control: Crime and Social Order in Contemporary Society.* Oxford University Press, 2001.

[314] A. Giddens, *The Consequences of Modernity*, 1st ed. Stanford, CA: Stanford University Press, 1991.

[315] R. B. Korobkin and T. S. Ulen, "Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics," *California Law Review*, vol. 88, no. 4, pp. 1051–1144, 2000.

[316] A. Acquisti, "The Economics of Personal Data and the Economics of Privacy," Tech. Rep., 2010. [Online]. Available: http://repository.cmu.edu/heinzworks/332

[317] S. Jacques and D. M. Reynald, "The Offenders' Perspective on Prevention," *Journal of Research in Crime and Delinquency*, vol. 49, no. 2, pp. 269–294, may 2012. [Online]. Available: http://journals.sagepub.com/doi/10.1177/0022427811408433

[318] R. Floyd, "Human Security and the Copenhagen School's Securitization Approach: Conceptualizing Human Security as a Securitizing Move," *Human Security Journal*, vol. 5, no. 37, pp. 38–49, 2007.

[319] D. R. Thomas, S. Pastrana, A. Hutchings, R. Clayton, and A. R. Beresford, "Ethical issues in research using datasets of illicit origin," in *Proceedings of the 2017 Internet Measurement Conference*. New York, NY: ACM Press, 2017, pp. 445–462. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3131365.3131389

[320] A. Hutchings and T. J. Holt, "A Crime Script Analysis of the Online Stolen Data Market," *British Journal of Criminology*, vol. 55, no. 3, pp. 596–614, 2015. [Online]. Available: http://bjc.oxfordjournals.org/lookup/doi/10.1093/bjc/azu106

[321] C. D. Marcum, G. E. Higgins, M. L. Ricketts, and T. L. Freiburger, "An Assessment of the Training and Resources Dedicated Nationally to Investigation of the Production of Child Pornography," *Policing*, vol. 5, no. 1, pp. 23–32, jan 2011. [Online]. Available: http://policing.oxfordjournals.org/cgi/doi/10.1093/police/paq057

[322] M. Innes, "Investigation order and major crime inquiries," in *Handbook of Criminal Investigation*, T. Newburn, T. Williamson, and A. Wright, Eds. Willan Publishing, 2007, ch. 10, pp. 255–276.

[323] A. Broeders, "Principles of forensic identification science," in *Handbook of Criminal Investigation*, T. Newburn, T. Williamson, and A. Wright, Eds. Willan Publishing, 2007, ch. 12, pp. 303–337.

[324] M. E. Badar and I. Marchuk, "A Comparative Study of the Principles Governing Criminal Responsibility in the Major Legal Systems of the World (England, United States, Germany, France, Denmark, Russia, China, and Islamic legal tradition)," *Criminal Law Forum*, vol. 24, no. 1, pp. 1–48, mar 2013. [Online]. Available: http://link.springer.com/10.1007/s10609-012-9187-z

[325] S. W. Brenner, “Is There Such a Thing as "Virtual Crime"?” *California Criminal Law Review*, vol. 4, no. 1, 2001. [Online]. Available: http://scholarship.law.berkeley.edu/bjcl/vol4/iss1/3

[326] A. R. Dick, “When does organized crime pay? A transaction cost analysis,” *International Review of Law and Economics*, vol. 15, no. 1, pp. 25–45, jan 1995. [Online]. Available: http://www.sciencedirect.com/science/article/pii/014481889400010R

[327] C. Cimpanu, “Dark Web Marketplace Launches Bug Bounty Program with $10,000 Rewards,” feb 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/dark-web-marketplace-launches-bug-bounty-program-with-10-000-rewards/

[328] I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” in *2013 IEEE Symposium on Security and Privacy.* IEEE, may 2013, pp. 397–411. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6547123

[329] M. Moser, R. Bohme, and D. Breuker, “An inquiry into money laundering tools in the Bitcoin ecosystem,” in *eCrime Researchers Summit, eCrime.* San Francisco, CA: IEEE Computer Society, 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6805780/

[330] C. Brenig, R. Accorsi, and G. Müller, “Economic Analysis of Cryptocurrency Backed Money Laundering,” in *ECIS 2015 Completed Research Papers*, vol. paper 20, Munster, may 2015. [Online]. Available: https://aisel.aisnet.org/ecis2015{_}cr/20

[331] C. Fijnaut, F. Bovenkerk, G. Bruinsma, and H. van de Bunt, *Organized Crime in the Netherlands.* The Hague / London / Boston: Kluwer Law International, 1998.

[332] C. J. C. F. Fijnaut, F. Bovenkerk, G. J. N. Bruinsma, and H. G. van de Bunt, “Eindrapport georganiseerde criminaliteit in Nederland,” WODC, Den Haag, Tech. Rep., 1995.

[333] Tweede Kamer der Staten-Generaal, “Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden),” Vergaderjaar 1996-1997. [Online]. Available: https://zoek.officielebekendmakingen.nl/kst-25403-3.html

[334] ——, “Memorie van Toelichting Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III),” Vergaderjaar 2015-2016. [Online]. Available: https://zoek.officielebekendmakingen.nl/kst-34372-3.html

[335] Council of Europe, "Explanatory Report to the Convention on Cybercrime," Budapest, 2001.

[336] B. Baker and A. Chiu, "Threat Spotlight: Rombertik - Gazing Past the Smoke, Mirrors, and Trapdoors," may 2015. [Online]. Available: https://blogs.cisco.com/security/talos/rombertik

[337] J. Fokker, R. Samani, and B. Potter, "No Ransomware: How Europol, Dutch Police & AWS Deal with Cybercrime (SAC327)," in *AWS re:Invent 2016*. Amazon Web Services, 2016. [Online]. Available: https://www.youtube.com/watch?v=HWYsoJvcWBE

[338] S. Hanford, "Thoughts on DarkSeoul: Data Sharing and Targeted Attackers," mar 2013. [Online]. Available: https://blogs.cisco.com/security/thoughts-on-darkseoul-data-sharing-and-targeted-attackers

[339] B. Krebs, "SpyEye, ZeuS Users Target Tracker Sites," 2011. [Online]. Available: http://krebsonsecurity.com/2011/03/spyeye-zeus-users-target-tracker-sites/{#}more-8520

[340] M. Deflem and J. E. Shutt, "Law Enforcement and Computer Security Threats and Measures," in *The Handbook of Information Security Volume 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations*, H. Bidgoli, Ed. Hoboken, NJ: John Wiley & Sons, 2006, pp. 200–209.

[341] K. W. Dam, H. S. Lin, Committee to Study National Cryptography Policy Computer Science and Telecommunications Board Commission on Physical Sciences, Mathematics, and Applications, *Cryptography's Role in Securing the Information Society.* Washington, D.C.: National Academy Press, 1996. [Online]. Available: https://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society

[342] R. L. Keeney, "Common Mistakes in Making Value Trade-Offs," *Operations Research*, vol. 50, no. 6, pp. 935–945, dec 2002. [Online]. Available: http://pubsonline.informs.org/doi/abs/10.1287/opre.50.6.935.357

[343] B. Krebs, "'Project Blitzkrieg' Promises More Aggressive Cyberheists Against U.S. Banks," oct 2012. [Online]. Available: https://krebsonsecurity.com/2012/10/project-blitzkrieg-promises-more-aggressive-cyberheists-against-u-s-banks/

[344] C. Engel, "The role of law in the governance of the internet," *International Review of Law, Computers & Technology*, vol. 20, no. 1-2, pp. 201–216, mar 2006. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/13600860600705101

[345] C. Hargreaves and D. Prince, "Understanding Cyber Criminals and Measuring Their Future Activity. Developing cybercrime research," Security Lancaster. Lancaster University, Tech. Rep., 2013.

[346] Rb. Rotterdam, “ECLI:NL:RBROT:2013:BZ4672,” 2013. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2013:BZ4672

[347] Rb. Gelderland, “ECLI:NL:RBGEL:2014:7698,” 2014. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBGEL:2014:7698

[348] Rb. Rotterdam, “ECLI:NL:RBROT:2016:5814,” jul 2016. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2016:5814

[349] Huawei, “Report Vulnerabilities.” [Online]. Available: http://www.huawei.com/en/psirt/report-vulnerabilities

[350] C. Kelk, *Studieboek materieel strafrecht*, 2nd ed. Deventer: Gouda Quint, 2001.

[351] B. Schneier, *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, 2003.

[352] Z. Dong, V. Garg, L. J. Camp, and A. Kapadia, “Pools, clubs and security,” in *Proceedings of the 2012 workshop on New security paradigms*. New York, New York, USA: ACM Press, sep 2012, p. 77. [Online]. Available: http://dl.acm.org/citation.cfm?id=2413296.2413304

[353] L. J. Camp, “Reconceptualizing the Role of Security User,” *Daedalus*, vol. 140, no. 4, pp. 93–107, oct 2011. [Online]. Available: http://www.mitpressjournals.org/doi/abs/10.1162/DAED{_}a{_}00117

[354] D. R. Johnson, S. P. Crawford, and J. G. Palfrey, “The Accountable Internet: Peer Production of Internet Governance,” *Virginia Journal of Law and Technology*, vol. 9, no. 97, pp. 1–33, 2004.

[355] H. Engerer, “Security Economics: Definition and Capacity,” 2009. [Online]. Available: https://core.ac.uk/download/pdf/6745583.pdf

[356] S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet,” *Northwestern Journal of Technology and Intellectual Property*, vol. 12, no. 1, pp. 1–66, 2014. [Online]. Available: http://heinonline.org/HOL/Page?handle=hein.journals/nwteintp12{&}id=1{&}div={&}collection=

[357] R. Wash and J. K. MacKie-Mason, “Security when people matter: structuring incentives for user behavior,” in *Proceedings of the ninth international conference on Electronic commerce*. New York, NY: ACM Press, 2007, pp. 7–14. [Online]. Available: http://dl.acm.org/citation.cfm?doid=1282100.1282105

[358] D. Turovsky, "America's hunt for Russian hackers: How FBI agents tracked down four of the world's biggest cyber-criminals and brought them to trial in the U.S." sep 2017. [Online]. Available: https://meduza.io/en/feature/2017/09/19/america-s-hunt-for-russian-hackers

[359] K. Poulsen, "Russia Issues International Travel Advisory to Its Hackers," sep 2013. [Online]. Available: https://www.wired.com/2013/09/dont-leave-home/

[360] S. Thielman and S. Ackerman, "US charges two Russian spies and two hackers in Yahoo data breach," 2017. [Online]. Available: https://www.theguardian.com/technology/2017/mar/15/fbi-charges-two-russian-spies-hackers-yahoo-data-breach

[361] Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," 2017. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

[362] M. Schwirtz and J. Goldstein, "Russian Espionage Piggybacks on a Cybercriminal's Hacking," mar 2017. [Online]. Available: https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html

[363] J. N. Martin and T. K. Nakayama, *Experiencing Intercultural Communication: An Introduction*, 5th ed. McGraw-Hill, 2014.

[364] J. Lusthaus and F. Varese, "Offline and Local: The Hidden Face of Cybercrime," *Policing: A Journal of Policy and Practice*, pp. 1–11, jul 2017. [Online]. Available: https://academic.oup.com/policing/article-lookup/doi/10.1093/police/pax042

[365] C. Herley and D. Florêncio, "A Profitless Endeavor: Phishing as Tragedy of the Commons," in *Proceedings of the 2008 workshop on New security paradigms*. New York, NY: ACM Press, aug 2008, p. 59. [Online]. Available: http://dl.acm.org/citation.cfm?id=1595676.1595686

[366] B. Krebs, "Meet Paunch: The Accused Author of the BlackHole Exploit Kit," dec 2013. [Online]. Available: https://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/

[367] L. Terrelonge III, "Cybercrime Economy. An Analysis of Criminal Communications Strategies," Flashpoint, Tech. Rep., 2017.

[368] S. Afroz, V. Garg, D. McCoy, and R. Greenstadt, "Honor among thieves: A common's analysis of cybercrime economies," in *eCrime Researchers Summit*. San Francisco, CA: IEEE, sep 2013, pp. 1–11. [Online]. Available: http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=6805778

[369] D. J. Teece, "Capturing Value From Knowledge Assets: The New Economy, Markets For Know-How, And Intangible Assets," *California Management Review*, vol. 40, no. 3, pp. 55–79, 1998.

[370] R. S. Kaplan and D. P. Norton, "Measuring the Strategic Readiness of Intangible Assets," *Harvard Business Review*, vol. 82, no. 2, pp. 33–46, 2004.

[371] N. Bontis, N. C. Dragonetti, K. Jacobsen, and G. Roos, "The knowledge toolbox: A Review of the Tools Available To Measure and Manage Intangible Resources," *European Management Journal*, vol. 17, no. 4, pp. 391–402, aug 1999. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0263237399000195

[372] B. Carrier and E. Spafford, "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[373] B.-J. Koops, "Police investigations in Internet open sources: Procedural-law issues," *Computer Law and Security Review*, vol. 29, no. 6, pp. 654–665, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.clsr.2013.09.004

[374] J. J. Oerlemans, "Hacken als opsporingsbevoegdheid," *Delikt & Delinkwent*, vol. 8, no. 62, pp. 888–908, 2011.

[375] O. S. Kerr, "Digital Evidence and the New Criminal Procedure," *Columbia Law Review*, vol. 105, no. 1, pp. 279–318, 2005. [Online]. Available: https://www.jstor.org/stable/4099310

[376] Y. G. Zabyelina, "Reverse money laundering in Russia: clean cash for dirty ends," *Journal of Money Laundering Control*, vol. 18, no. 2, pp. 202–219, 2015.

[377] M. van den Abeele, "THTC op de crime scene. Een onderzoek naar het hanteren van een plaats delict en/of een doorzoeking door THTC ten behoeve van fysieke sporen." 2017.

[378] L. Kaufmann and Y. Schneider, "Intangibles: A synthesis of current research," *Journal of Intellectual Capital*, vol. 5, no. 3, pp. 366–388, sep 2004. [Online]. Available: http://www.emeraldinsight.com/doi/abs/10.1108/14691930410550354

[379] N. Bontis, "Assessing knowledge assets: a review of the models used to measure intellectual capital," *International Journal of Management Reviews*, vol. 3, no. 1, pp. 41–60, 2001.

[380] R. Nolker and L. Zhou, "Social Computing and Weighting to Identify Member Roles in Online Communities," in *The 2005 IEEE/WIC/ACM International Conference on Web Intelligence.* Compiegne, France:

IEEE, 2005, pp. 87–93. [Online]. Available: http://ieeexplore.ieee.org/document/1517823/

[381] V. Allee, “Value network analysis and value conversion of tangible and intangible assets,” *Journal of Intellectual Capital*, vol. 9, no. 1, pp. 5–24, apr 2008. [Online]. Available: http://www.emeraldinsight.com/doi/abs/10.1108/14691930810845777

[382] L. Allodi, F. Massacci, and J. M. Williams, “The Work-Averse Cyber Attacker Model: Theory and Evidence From Two Million Attack Signatures,” in *Workshop on the Economics of Information Security*, San Diego, CA, jun 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=2862299

[383] Landelijke Eenheid, “Opnieuw aanhoudingen voor leveren crypto-gsm’s aan onderwereld,” may 2017. [Online]. Available: https://www.politie.nl/nieuws/2017/mei/10/11-opnieuw-aanhoudingen-voor-leveren-crypto-gsm’s-aan-onderwereld.html

[384] M. Taylor, E. Quayle, and G. Holland, “Child Pornography: The Internet and Offending,” *Canadian Journal of Policy Research*, vol. 2, no. 2, pp. 94–100, 2001.

[385] K. V. Acar, “Child abuse materials as digital goods: Why we should fear new commercial forms,” 2017. [Online]. Available: https://www.econstor.eu/handle/10419/157247

[386] D. Lyon, “An Electronic Panopticon? A Sociological Critique of Surveillance Theory,” *The Sociological Review*, vol. 41, no. 4, pp. 653–678, nov 1993. [Online]. Available: http://journals.sagepub.com/doi/10.1111/j.1467-954X.1993.tb00896.x

[387] M. Goncharov, “Russian Underground 101,” Trend Micro, Tech. Rep., 2012. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

[388] ——, “Russian Underground Revisited,” Trend Micro, Tech. Rep., 2014. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

[389] The European Financial Coalition against commercial sexual exploitation of children online, “14 months on: A combined report from the European Financial Coalition 2009-2010,” Tech. Rep., 2010.

[390] D. Verlaan and J. Wetzels, “Gevaarlijk pedohandboek ongestoord verspreid via internet, politiek wil verbod,” mar 2018. [Online]. Available: https://www.rtlnieuws.nl/nederland/gevaarlijk-pedohandboek-ongestoord-verspreid-via-internet-politiek-wil-verbod?{_}sp=e45e5334-a7cf-4ebe-b5ab-28fac7a6967a.1522399233082

[391] M. van Dantzig, D. Heppener, F. Ruiz, Y. Klijnsma, Y. Z. Hu, E. de Jong, K. de Mik, and L. Haagsma, “Ponmocup. A giant hiding in the shadows,” Fox-IT, Tech. Rep., 2015. [Online]. Available: https://foxitsecurity.files.wordpress.com/2015/12/foxit-whitepaper{_}ponmocup{_}1{_}1.pdf

[392] B. H. Schell, M. V. Martin, P. C. Hung, and L. Rueda, “Cyber child pornography: A review paper of the social and legal issues and remedies - and a proposed technological solution,” *Aggression and Violent Behavior*, vol. 12, no. 1, pp. 45–63, jan 2007. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1359178906000401

[393] G. Borisevich, N. Chernyadyeva, E. Frolovich, P. Pastukhov, S. Polyakova, O. Dobrovlyanina, D. G. Keeling, and M. M. Losavio, “A comparative review of cybercrime law and digital forensics in Russia, the United States and under the convention on cybercrime of the Council of Europe,” *Northern Kentucky Law Review*, vol. 39, no. 2, pp. 267–326, 2012.

[394] Q. Wang, “A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe,” Ph.D. dissertation, Erasmus Universiteit Rotterdam, 2016.

[395] B. Krebs, “Deleted Facebook Cybercrime Groups Had 300,000 Members,” apr 2018. [Online]. Available: https://krebsonsecurity.com/2018/04/deleted-facebook-cybercrime-groups-had-300000-members/

[396] R. Stoyanov, “Russian financial cybercrime: how it works,” nov 2015. [Online]. Available: https://securelist.com/russian-financial-cybercrime-how-it-works/72782/

[397] R. Schoemaker, “TorRAT-bende anoniem door gebruik VPN en Bitcoins,” oct 2013. [Online]. Available: http://computerworld.nl/security/79823-torrat-bende-anoniem-door-gebruik-vpn-en-bitcoins

[398] L. Constantin, “Cybercrime service automates creation of fake ID verification documents,” aug 2013. [Online]. Available: https://www.pcworld.com/article/2047559/cybercrime-service-automates-creation-of-fake-scanned-ids-other-identity-verification-documents.html

[399] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, “Measuring pay-per-install: the commoditization of malware distribution,” in *Proceedings of the 20th USENIX conference on Security*. San Francisco, CA: USENIX Association, 2011, pp. 1–13. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028080

[400] B. Krebs, “’AntiDetect’ Helps Thieves Hide Digital Fingerprints,” mar 2015. [Online]. Available: https://krebsonsecurity.com/2015/03/antidetect-helps-thieves-hide-digital-fingerprints/

[401] J. Kirk, “This tool may make it easier for thieves to empty bank accounts,” jan 2015. [Online]. Available: https://www.computerworld.com/article/2871926/this-tool-may-make-it-easier-for-thieves-to-empty-bank-accounts.html

[402] J. Simpson and E. Weiner, “Money laundering,” in *Oxford English Dictionary.* Oxford: Oxford University Press, 1989.

[403] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, “Mixcoin: Anonymity for Bitcoin with accountable mixes,” in *Financial Cryptography and Data Security: 18th International Conference.*, N. Christin and R. Safavi-Naini, Eds., vol. 8437. Christ Church, Barbados: Springer, 2014, pp. 486–504. [Online]. Available: http://eprint.iacr.org/2014/077/20140204:170311

[404] Team Cymru, “The Future of Passports and Money Movement in the Underground Economy,” Tech. Rep., 2010. [Online]. Available: http://www.team-cymru.com/ReadingRoom/Whitepapers/2010/FakeID{_}in{_}the{_}Underground{_}Economy.pdf

[405] J. Yaffa, “The Double Sting. A power struggle between Russia’s rival security agencies.” jul 2015. [Online]. Available: https://www.newyorker.com/magazine/2015/07/27/the-double-sting

[406] J. Mullin, “Corrupt Silk Road investigator pleads guilty, admits to $240K movie deal,” 2015. [Online]. Available: http://arstechnica.com/tech-policy/2015/07/corrupt-silk-road-agent-pleads-guilty/

[407] T. W. van Boheemen, “De aangiftebereidheid van burgers met betrekking tot cybercrime,” 2017.

[408] V. van der Boon, “OM: beperk verschoningsrecht advocaat en notaris,” 2015. [Online]. Available: https://fd.nl/economie-politiek/1108196/openbaar-ministerie-beperk-verschoningsrecht-advocaat-en-notaris

[409] F. Mercês, “The Brazilian Underground Market: The Market for Cybercriminal Wannabes?” Trend Micro, Tech. Rep., 2014. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf

[410] T. Morrison, “Botnet Controllers in the Cloud,” apr 2017. [Online]. Available: https://www.spamhaus.org/news/article/736/botnet-controllers-in-the-cloud

[411] W. Heck, “Het Openbaar Ministerie bagatelliseerde brand bij Vodafone,” 2015. [Online]. Available: http://www.nrc.nl/nieuws/2015/02/14/het-openbaar-ministerie-bagatelliseerde-brand-bij-vodafone/

[412] B. Hayes, J. Jeandesboz, F. Ragazzi, S. Simon, and V. Mitsilegas, "The law enforcement challenges of cybercrime: are we really playing catch-up?" European Parliament. Policy Department Citizens' Rights and Constitutional Affairs, Brussels, Tech. Rep., 2015. [Online]. Available: http://www.europarl.europa.eu/studies

[413] S. Huisman, M. Princen, P. Klerks, and N. Kop, "Handelen naar waarheid Sterkte- en zwakteanalyse van de opsporing," Politieacademie, Apeldoorn, Tech. Rep., 2016.

[414] Eurojust, "Operation BlackShades. An Evaluation," Eurojust, Tech. Rep., 2015. [Online]. Available: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/OperationBlackshades-Anevaluation(April2015)/2015-04{_}Blackshades-Case{_}EN.pdf

[415] L. van Hout, "Samen slimmer tegen cybercrime. Good practices uit het onderzoek Rootkit." Landelijke Eenheid/Dienst Landelijke Recherche/Team High Tech Crime, Tech. Rep., 2015.

[416] M. Sandee, "GameOver ZeuS: Badguys and Backends," Fox-IT, Tech. Rep., 2015. [Online]. Available: https://www.fox-it.com/en/files/2015/08/FoxIT-Whitepaper{_}Blackhat-web.pdf

[417] NATO Cooperative Cyber Defence Centre of Excellence, "NotPetya and WannaCry Call for a Joint Response from International Community," 2017. [Online]. Available: https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html

[418] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn: NATO CCD COE Publications, 2015, ch. 9, pp. 79–86.

[419] F-Secure Labs Security Response, "BlackEnergy & Quedagh. The convergence of crimeware and APT attacks," F-Secure, Tech. Rep., 2014. [Online]. Available: https://www.f-secure.com/documents/996508/1030745/blackenergy{_}whitepaper.pdf

[420] G. Guzman, "Hiding in Plain Sight: The Growth of Cybercrime in Social Media (Part 2)," RSA, Tech. Rep., 2016. [Online]. Available: https://www.rsa.com/en-us/resources/hiding-in-plain-sight-part-2

[421] RSA, "Hiding in Plain Sight: The Growth of Cybercrime in Social Media (Part 1)," RSA, Tech. Rep., 2016. [Online]. Available: https://www.rsa.com/content/dam/en/white-paper/hiding-in-plain-sight-the-growth-of-cybercrime-in-social-media-part-1.pdf

[422] B. Fung, "How Microsoft killed off a massive botnet, with trademark law," jul 2013. [Online]. Available: https://www.washingtonpost.com/news/wonk/wp/2013/07/24/how-microsoft-killed-off-a-massive-botnet-with-trademark-law/?utm{_}term=.cf8e40260d07

[423] J. Meisner, "Microsoft Names Defendants in Zeus Botnets Case; Provides New Evidence to FBI," jul 2012. [Online]. Available: https://blogs.microsoft.com/blog/2012/07/02/microsoft-names-defendants-in-zeus-botnets-case-provides-new-evidence-to-fbi/

[424] R. D. Boscovich, "Microsoft Reaches Settlement with Piatti, dotFREE Group in Kelihos Case," oct 2011. [Online]. Available: https://blogs.microsoft.com/blog/2011/10/26/microsoft-reaches-settlement-with-piatti-dotfree-group-in-kelihos-case/

[425] N. Wingfield and N. Perlroth, "Microsoft Raids Tackle Internet Crime," mar 2012. [Online]. Available: http://www.nytimes.com/2012/03/26/technology/microsoft-raids-tackle-online-crime.html

[426] B. Krebs, "Who is Anna-Senpai, the Mirai Worm Author?" jan 2017. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

[427] Shadowserver Foundation, "Shadowserver Foundation - Stats - Sinkholes," 2018. [Online]. Available: https://www.shadowserver.org/wiki/pmwiki.php/Stats/Sinkholes

[428] V. Benjamin, W. Li, T. Holt, and H. Chen, "Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops," in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, may 2015, pp. 85–90. [Online]. Available: http://ieeexplore.ieee.org/document/7165944/

[429] C. Fachkha and M. Debbabi, "Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7317717/

[430] B. Thompson, "UK data protection rules to exempt journalists and researchers," sep 2017. [Online]. Available: https://www.ft.com/content/888e94dc-98a0-11e7-b83c-9588e51488a0

[431] D. Décary-Hétu and B. Dupont, "Reputation in a dark network of online criminals," *Global Crime*, vol. 14, no. 2-3, pp. 175–196, 2013. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/17440572.2013.801015

[432] D. Palotay, "Ransomware as a service: how the bad guys marketed Philadelphia," Sophos, Tech. Rep., 2017. [Online]. Available: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/RaaS-Philadelphia.pdf

[433] D. Stama, "Rombertik is CarbonGrabber with a sting in the tail for cheapskates," may 2015. [Online]. Available: http://www.symantec.com/connect/blogs/rombertik-carbongrabber-sting-tail-cheapskates

[434] B. Krebs, “SpyEye v. ZeuS Rivalry Ends in Quiet Merger,” oct 2010. [Online]. Available: https://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/

[435] H. Fraser, “Exploring the Blackhole Exploit Kit,” SophosLabs UK, Tech. Rep., 2012. [Online]. Available: https://sophosnews.files.wordpress.com/2012/03/blackhole{_}paper{_}mar2012.pdf

[436] K. K. e Silva, “Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?” *International Review of Law, Computers & Technology*, pp. 1–16, dec 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/13600869.2018.1418142

[437] Hoge Raad der Nederlanden, “ECLI:NL:HR:2003:AE9038,” jan 2003. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2003:AE9038

[438] ——, “ECLI:NL:HR:2008:BA8179,” mar 2008. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2008:BA8179

[439] A. Chen, “Elaborate Anonymous Sting Snags 190 Kiddie Porn Fans,” 2011. [Online]. Available: http://gawker.com/5855604/elaborate-anonymous-sting-snags-190-kiddie-porn-fans

[440] Group-IB, “MoneyTaker. 1.5 years of silent operations,” Group-IB, Tech. Rep., 2017. [Online]. Available: https://www.group-ib.com/resources/threat-research/money-taker.html

[441] Rb. Rotterdam, “ECLI:NL:RBROT:2014:7379,” 2014. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2014:7379

[442] Group-IB, “Cron has fallen,” may 2017. [Online]. Available: https://www.group-ib.com/blog/cron

[443] Associated Press, “Russian agents, hackers charged in massive Yahoo breach,” 2017. [Online]. Available: http://www.dailymail.co.uk/wires/ap/article-4316514/US-expected-announce-charges-related-Yahoo-data-breach.html

[444] B. Wheeler, “EU could turn to ’crowd sourcing’ in cyber crime fight,” dec 2010. [Online]. Available: http://www.bbc.com/news/mobile/uk-politics-12004134

[445] B. Krebs, “Who Is Marcus Hutchins?” sep 2017. [Online]. Available: https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/

[446] V. van Mieghem and J. Pouwelse, “Anonymous online purchases with exhaustive operational security,” *eprint arXiv:1505.07370*, 2015. [Online]. Available: http://adsabs.harvard.edu/abs/2015arXiv150507370V

[447] S. Kravchenko, C. Matlack, and D. Lawrence, “Biggest U.S. hacking case is tale of gamers’ interrupted vacation,” mar 2015. [Online]. Available: https://www.bloomberg.com/news/articles/2015-01-12/biggest-u-s-hack-case-is-tale-of-gamers-interrupted-vacation

[448] M. Willacy, “Detectives took on paedophile’s identity in ’dark net’ abuse sting,” aug 2015. [Online]. Available: http://www.abc.net.au/news/2015-08-26/secret-anti-paedophile-operation-saves-children-from-abuse/6720304

[449] N. A. Karlova and J. H. Lee, “Notes from the underground city of disinformation: A conceptual investigation,” *Proceedings of the American Society for Information Science and Technology*, vol. 48, no. 1, pp. 1–9, jan 2011. [Online]. Available: http://doi.wiley.com/10.1002/meet.2011.14504801133

[450] N. A. Karlova and K. E. Fisher, “A social diffusion model of misinformation and disinformation for understanding human information behaviour,” *Information Research*, vol. 18, no. 1, pp. 1–17, 2013. [Online]. Available: http://www.informationr.net/ir/18-1/paper573.html

[451] G. A. Akerlof, “The Market for "Lemons": Quality Uncertainty and the Market Mechanism,” *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, 1970. [Online]. Available: http://www.jstor.org/stable/1879431?seq=1{#}page{_}scan{_}tab{_}contents

[452] M. Yip, C. Webber, and N. Shadbolt, “Trust among cybercriminals? Carding forums, uncertainty and implications for policing,” *Policing and Society*, vol. 23, no. 4, pp. 516–539, dec 2013. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/10439463.2013.780227

[453] T. J. Holt, O. Smirnova, and A. Hutchings, “Examining signals of trust in criminal markets online,” *Journal of Cybersecurity*, vol. 2, no. 2, pp. 137–145, 2016. [Online]. Available: https://cybersecurity.oxfordjournals.org/content/early/2016/09/14/cybsec.tyw007.abstract

[454] L. Allodi, M. Corradin, and F. Massacci, “Then and Now: On the Maturity of the Cybercrime Markets The Lesson That Black-Hat Marketeers Learned,” *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 35–46, jan 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7044581/

[455] B. Krebs, “Ragebooter: ’Legit’ DDoS Service, or Fed Backdoor?” may 2013. [Online]. Available: https://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor/

[456] Y. J. Fanusie and T. Robinson, “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services,” oundation for Defense of Democracies’ Center on Sanctions and Illicit Finance, Tech. Rep., 2018.

[Online]. Available: http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-bitcoin-laundering/

[457] R. Anderson, I. Shumailov, and M. Ahmed, “Making Bitcoin Legal,” 2018. [Online]. Available: http://www.cl.cam.ac.uk/{~}rja14/Papers/making-bitcoin-legal.pdf

[458] D. Adrian, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin, P. Zimmermann, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, and E. Thomé, “Imperfect Forward Secrecy,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. New York, NY: ACM Press, oct 2015, pp. 5–17. [Online]. Available: http://dl.acm.org/citation.cfm?id=2810103.2813707

[459] HostExploit, “Top 50 Bad Hosts and Networks 4th Quarter 2010,” Tech. Rep., 2011. [Online]. Available: http://hostexploit.com/downloads/top{_}50{_}bad{_}hosts{_}201012.pdf

[460] Platform Internetveiligheid, “Notice-and-take-down. Code of conduct. Version 1.” ECP, Tech. Rep., 2008. [Online]. Available: https://ecp.nl/sites/default/files/NTD{_}Gedragscode{_}Engels.pdf

[461] V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi, and A. Mei, “A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients,” *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 1, pp. 77–91, jan 2015. [Online]. Available: http://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015-0006/popets-2015-0006.xml?ncid=txtlnkusaolp00000618

[462] D. P. Biros, J. F. George, and R. W. Zmud, “Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study,” *MIS Quarterly*, vol. 26, no. 2, pp. 119–144, 2002.

[463] P. E. Johnson, S. Grazioli, and K. Jamal, “Fraud detection: Intentionality and deception in cognition,” *Accounting, Organizations and Society*, vol. 18, no. 5, pp. 467–488, jul 1993. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0361368293900425

[464] R. C. Newman, “Cybercrime, identity theft, and fraud,” in *Proceedings of the 3rd annual conference on Information security curriculum development*. New York, NY: ACM Press, sep 2006, p. 68. [Online]. Available: https://dl.acm.org/citation.cfm?id=1231064

[465] C. Txe-wei and L. Wu, “Civic-minded residents, ubiquitous cameras help crack ATM case,” jul 2016. [Online]. Available: http://focustaiwan.tw/news/asoc/201607180021.aspx

[466] S. Grazioli and S. L. Jarvenpaa, "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *International Journal of Electronic Commerce*, vol. 7, no. 4, pp. 93–118, dec 2014. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/10864415.2003.11044283

[467] J. Yuill, D. E. Denning, and F. Feer, "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques," *Journal of Information Warfare*, vol. 5, no. 3, pp. 26–40, 2006. [Online]. Available: http://oai.dtic.mil/oai/oai?verb=getRecord{&}metadataPrefix=html{&}identifier=ADA485003

[468] W. W. Martin, "Honey Pots and Honey Nets - Security through Deception," 2001. [Online]. Available: http://www.sans.org/reading-room/whitepapers/attacking/honey-pots-honey-nets-security-deception-41

[469] M. Nohlberg and S. Kowalski, "The cycle of deception: a model of social engineering attacks, defenses and victims," in *Second International Symposium on Human Aspects of Information Security and Assurance*, N. Clarke and S. Furnell, Eds. Plymouth, UK: University of Plymouth, 2008, pp. 1–11. [Online]. Available: http://www.diva-portal.org/smash/record.jsf?pid=diva2{%}3A291309{&}dswid=1793

[470] S. Grazioli and S. L. Jarvenpaa, "Deceived: Under Target Online," *Communications of the ACM*, vol. 46, no. 12, pp. 196–205, dec 2003. [Online]. Available: http://dl.acm.org/ft{_}gateway.cfm?id=953500{&}type=html

[471] N. C. Rowe and E. J. Custy, "Deception in Cyber Attacks," in *Cyber Warfare and Cyber Terrorism*, L. Janczewski and A. Colarik, Eds. IGI Global, 2007, ch. 12, pp. 91–97. [Online]. Available: https://calhoun.nps.edu/handle/10945/36422

[472] P. E. Johnson, S. Grazioli, K. Jamal, and R. G. Berryman, "Detecting deception: adversarial problem solving in a low base-rate world," *Cognitive Science*, vol. 25, no. 3, pp. 355–392, may 2001. [Online]. Available: http://doi.wiley.com/10.1207/s15516709cog2503{_}2

[473] J. Wolak, D. Finkelhor, and K. Mitchell, "Internet-initiated sex crimes against minors: implications for prevention based on findings from a national study." *The Journal of adolescent health*, vol. 35, no. 5, pp. 11–20, nov 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1054139X04001715

[474] Damballa, "PonyUp: Tracing Pony's Threat Cycle and Multi-Stage Infection Chain," Tech. Rep., 2015. [Online]. Available: https://www.damballa.com/wp-content/uploads/2015/08/Damballa{_}PonyUp.pdf

[475] J. B. Bell and B. Whaley, *Cheating and Deception*, 3rd ed. Transaction Publishers, 2009.

[476] N. C. Rowe, "Deception in Defense of Computer Systems from Cyber Attack," in *Cyber Warfare and Cyber Terrorism*, L. Janczewski and A. Colarik, Eds. IGI Global, jan 2007, pp. 97–104. [Online]. Available: https://calhoun.nps.edu/handle/10945/36424

[477] A. Soldatov and I. Borogan, *The New Nobility. The Restoration of Russia's Security State and the Enduring Legacy of the KGB.* PublicAffairs, 2010.

[478] Associated Press, "'Anonymous' hacks thousands of credit card numbers from security firm... and gives money to charity," dec 2011. [Online]. Available: http://www.dailymail.co.uk/news/article-2078559/Anonymous-hacks-thousands-credit-card-numbers-security-firm--gives-money-charity.html

[479] R. Dremliuga, "Subculture of Hackers in Russia," *Asian Social Science*, vol. 10, no. 18, pp. 158–162, 2014.

[480] L. Zhao and M. Mannan, "Deceptive Deletion Triggers under Coercion," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2763–2776, 2016. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7536120

[481] M. Brennan and R. Greenstadt, "Practical Attacks Against Authorship Recognition Techniques," in *Proceedings of the Twenty-First Conference on Innovative Applications of Artificial Intelligence (IAAI)*, Pasadena, CA, 2009.

[482] W. Mazurczyk and L. Caviglione, "Information Hiding as a Challenge for Malware Detection," *IEEE Security & Privacy*, vol. 13, no. 2, pp. 89–93, mar 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7085644

[483] J. Franklin, V. Paxson, S. Savage, and A. Perrig, "An inquiry into the nature and causes of the wealth of internet miscreants," in *Proceedings of the 14th ACM conference on Computer and communications security.* New York, NY: ACM Press, oct 2007, pp. 375–388. [Online]. Available: http://dl.acm.org/citation.cfm?id=1315245.1315292

[484] R. J. Lewicki, D. J. McAllister, and R. J. Bies, "Trust and Distrust: New Relationships and Realities," *Academy of Management Review*, vol. 23, no. 3, pp. 438–458, jul 1998. [Online]. Available: http://amr.aom.org/content/23/3/438.full

[485] R. Mansell and B. S. Collins, "Introduction: Trust and crime in information societies," in *Trust and Crime in Information Societies*,

R. Mansell and B. S. Collins, Eds. Cheltenham, UK: Edward Elgar, feb 2005, ch. 1, pp. 1–10. [Online]. Available: http://eprints.lse.ac.uk/9000/1/Mansell{_}introduction{_}trust{_}crime{_}2005.pdf

[486] K. Thompson, "Reflections on trusting trust," *Communications of the ACM*, vol. 27, no. 8, pp. 761–763, aug 1984. [Online]. Available: http://dl.acm.org/citation.cfm?id=358198.358210

[487] T. Moore and N. Christin, "Beware the middleman: Empirical analysis of Bitcoin-exchange risk," in *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science*, A. R. Sadeghi, Ed., vol. 7859. Berlin, Heidelberg: Springer, 2013, pp. 25–33. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-39884-1{_}3

[488] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," in *Proceedings of the 2013 conference on Internet measurement conference.* New York, NY: ACM Press, oct 2013, pp. 127–140. [Online]. Available: http://dl.acm.org/citation.cfm?id=2504730.2504747

[489] J. Pearson and L. Franceschi-Bicchierai, "There's a Bitcoin Bounty Out on Those Alleged 'Evolution' Drug Market Scammers," 2015. [Online]. Available: https://motherboard.vice.com/en{_}us/article/theres-a-bitcoin-bounty-out-on-those-alleged-evolution-drug-market-scammers

[490] D. H. McKnight and N. Chervany, "While Trust is Cool and Collected, Distrust is Fiery and Frenzied: A Model of Distrust Concepts," in *Seventh Americas Conference on Information Systems*, D. Strong, D. Straub, and J. I. DeGross, Eds. Boston, MA: Omnipress, 2001, pp. 883–888. [Online]. Available: http://aisel.aisnet.org/amcis2001/171

[491] D. H. McKnight and N. L. Chervany, "Trust and Distrust Definitions: One Bite at a Time," in *Trust in Cyber-societies*, ser. Lecture Notes in Computer Science, R. Falcone, M. Singh, and Y.-H. Tan, Eds. Berlin, Heidelberg: Springer, dec 2001, pp. 22–54. [Online]. Available: http://link.springer.com/10.1007/3-540-45547-7

[492] N. Falliere, "Sality: Story of a Peer-to-Peer Viral Network," Symantec, Tech. Rep., 2011. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/sality-story-of-peer-to-peer-11-en.pdf

[493] G. A. Fine and L. Holyfield, "Secrecy, Trust, and Dangerous Leisure: Generating Group Cohesion in Voluntary Organizations," *Social Psychology Quarterly*, vol. 59, no. 1, pp. 22–38, 1996. [Online]. Available: http://www.jstor.org/stable/2787117?origin=crossref{&}seq=1{#}page{_}scan{_}tab{_}contents

[494] GReAT, "Tyupkin: manipulating ATM machines with malware," oct 2014. [Online]. Available: https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/

[495] B. Krebs, "Fool Me Once...," apr 2013. [Online]. Available: https://krebsonsecurity.com/2013/04/fool-me-once/

[496] Group-IB, "Cobalt: logical attacks on ATMs," Group-IB, Tech. Rep., 2016. [Online]. Available: https://www.group-ib.com/resources/threat-research/cobalt.html

[497] P. Coogan, "SpyEye Bot versus Zeus Bot," 2010. [Online]. Available: https://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot

[498] Redactie, "Oorlog tussen virusmakers lijkt ten einde," mar 2004. [Online]. Available: http://webwereld.nl/security/14348-oorlog-tussen-virusmakers-lijkt-ten-einde

[499] C. Osborne, "Crysis ransomware master keys released to the public," may 2017. [Online]. Available: http://www.zdnet.com/article/crysis-ransomware-master-keys-released-to-the-public/

[500] P. Stancik, "ESET releases new decryptor for TeslaCrypt ransomware," may 2016. [Online]. Available: https://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/

[501] A. Gupta, P. Kumaraguru, and A. Sureka, "Characterizing Pedophile Conversations on the Internet using Online Grooming," *arXiv*, vol. 1208.4324, 2012. [Online]. Available: https://arxiv.org/abs/1208.4324

[502] A. Aljaedi, D. Lindskog, P. Zavarsky, R. Ruhl, and F. Almari, "Comparative Analysis of Volatile Memory Forensics: Live Response vs. Memory Imaging," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*. Boston, MA: IEEE, oct 2011, pp. 1253–1258. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6113291

[503] M. Damshenas, A. Dehghantanha, R. Mahmoud, and S. bin Shamsuddin, "Forensics investigation challenges in cloud computing environments," in *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic*. Kuala Lumpur, Malaysia: IEEE, jun 2012, pp. 190–194. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6246092

[504] N. Beebe, "Digital forensic research: The good, the bad and the unaddressed," in *Advances in digital forensics V. Fifth IFIP WG 11.9 International Conference on Digital Forensics*, G. Peterson and S. Shenoi, Eds. Orlando, FL: Springer, 2009, pp. 17–36. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-04155-6{_}2

[505] J. Cheng, “Botnet master hits the kill switch, takes down 100,000 PCs,” aug 2009. [Online]. Available: https://arstechnica.com/information-technology/2009/05/zeus-botnet-hits-the-kill-switch-takes-down-100000-pcs/

[506] X. Shu, K. Tian, A. Ciambrone, and D. D. Yao, “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned,” *arXiv*, 2017. [Online]. Available: https://arxiv.org/pdf/1701.04940.pdf

[507] K. D. Haggerty, Richard V. Ericson and R. V. Ericson, “The surveillant assemblage,” *British Journal of Sociology*, vol. 51, no. 4, pp. 605–622, dec 2000. [Online]. Available: http://doi.wiley.com/10.1080/00071310020015280

[508] S. Lynch, “How Bad Guys Hide Online, Part One,” sep 2015. [Online]. Available: https://umbrella.cisco.com/blog/2015/09/11/how-bad-guys-hide-online-pt-one/

[509] B. Krebs, “Security Trade-Offs in the New EU Privacy Law,” apr 2018. [Online]. Available: https://krebsonsecurity.com/2018/04/security-trade-offs-in-the-new-eu-privacy-law/

[510] N. Biasini, “Bedep Lurking in Angler’s Shadows,” feb 2016. [Online]. Available: https://blogs.cisco.com/security/talos/bedep-actor

[511] J. Reardon, D. Basin, and S. Capkun, “On Secure Data Deletion,” *IEEE Security & Privacy*, vol. 12, no. 3, pp. 37–44, may 2014. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6678339

[512] Rb. ’s-Gravenhage, “ECLI:NL:RBSGR:2011:BR4524,” 2011. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBSGR:2011:BR4524

[513] ——, “ECLI:NL:RBSGR:2010:BO5163,” 2010. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBSGR:2010:BO5163

[514] Rb. Zutphen, “ECLI:NL:RBZUT:2010:BO8152,” 2010. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBZUT:2010:BO8152

[515] Rb. Midden-Nederland, “ECLI:NL:RBMNE:2013:3688,” 2013. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2013:3688

[516] Rb. Overijssel, “ECLI:NL:RBOVE:2016:671,” 2016. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBOVE:2016:671

[517] Rb. Amsterdam, “ECLI:NL:RBAMS:2008:BD2286,” 2008. [Online]. Available: https://uitspraken.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2008:BD2286

[518] B. Herzog and Y. Balmas, “Great Crypto Failures,” in *Virus Bulletin*, Denver, 2016. [Online]. Available: http://blog.checkpoint.com/wp-content/uploads/2016/10/GreatCryptoFailuresWhitepaper{_}Draft2.pdf

[519] Rb. Utrecht, “ECLI:NL:RBUTR:2012:BY7522,” 2012. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBUTR:2012:BY7522

[520] Hof Amsterdam, “ECLI:NL:GHAMS:2013:BZ8885,” 2013. [Online]. Available: https://uitspraken.rechtspraak.nl/uitspraak?id=ECLI:NL:GHAMS:2013:BZ8885

[521] Rb. Den Haag, “ECLI:NL:RBDHA:2014:15611,” 2014. [Online]. Available: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:15611

[522] N. Yamashita, V. Evers, C. Rosé, and M. B. Watson-Manheim, Eds., *Proceedings of the 5th ACM International Conference on Collaboration Across Boundaries: Culture, Distance & Technology.* New York, NY: ACM, 2014.

[523] R. Anderson and F. Stajano, “It’s the Anthropology, Stupid!” in *Security Protocols XVIII. Security Protocols 2010. Lecture Notes in Computer Science, vol 7061*, B. Christianson and J. Malcolm, Eds. Berlin, Heidelberg: Springer, 2014, pp. 127–130. [Online]. Available: https://www.cl.cam.ac.uk/{˜}rja14/Papers/hbac.pdf

[524] M. J. Bennett, “Intercultural communication: A current perspective.” in *Basic concepts of intercultural communication: Selected readings.*, M. J. Bennett, Ed. Yarmouth, ME: Intercultural Press, 1998.

[525] P. Paganini, “Large communities of Eastern Europe cybercriminals ’Verified’ hacked,” jan 2014. [Online]. Available: http://securityaffairs.co/wordpress/21120/cyber-crime/verified-communities-hacked.html

[526] Europol, “Cybercriminal Darkode forum taken down through global action,” 2015. [Online]. Available: https://www.europol.europa.eu/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action

[527] Trend Micro, “Cybercriminal Underground Economy Series.” [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series

[528] ——, “Brazilians in the Russian Underground,” jul 2014. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/brazilians-in-the-russian-underground/

[529] T. Bateman, “Police warning after drug traffickers’ cyber-attack,” oct 2013. [Online]. Available: http://www.bbc.com/news/world-europe-24539417

[530] J. M. Bennett, *The SAGE Encyclopedia of Intercultural Competence.* Sage, 2015.

[531] G. Hofstede, G. J. Hofstede, and M. Minkov, *Cultures and Organizations: Software of the Mind*, 3rd ed. McGraw-Hill USA, 2010.

[532] Trend Micro, “The Many Faces of Cybercrime,” 2016. [Online]. Available: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-many-faces-of-cybercrime

[533] A. Urano, “The Japanese Underground,” Trend Micro, Tech. Rep., 2015. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-japanese-underground.pdf

[534] A. Zanghellini, “Underage Sex and Romance in Japanese Homoerotic Manga and Anime,” *Social & Legal Studies*, vol. 18, no. 2, pp. 159–177, jun 2009. [Online]. Available: http://sls.sagepub.com/cgi/doi/10.1177/0964663909103623

[535] K. Hendley, “’Telephone Law’ and the ’Rule of Law’: The Russian Case,” *Hague Journal on the Rule of Law*, vol. 1, no. 02, pp. 241–262, sep 2009. [Online]. Available: http://www.journals.cambridge.org/abstract{_}S1876404509002413

[536] ——, “Varieties of Legal Dualism: Making Sense of the Role of Law in Contemporary Russia,” *Wisconsin International Law Journal*, vol. 29, no. 2, pp. 233–262, 2011. [Online]. Available: http://heinonline.org/HOL/Page?handle=hein.journals/wisint29{&}id=245{&}div={&}collection=

[537] ——, “Who Are the Legal Nihilists in Russia?” *Post-Soviet Affairs*, vol. 28, no. 2, pp. 149–186, apr 2012. [Online]. Available: http://bellwether.metapress.com/openurl.asp?genre=article{&}id=doi:10.2747/1060-586X.28.2.149

[538] N. Kostyuk, “Ukraine: A Cyber Safe Haven?” in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn: NATO CCD COE Publications, 2015, ch. 13, pp. 113–122.

[539] F. Varese, “The local dimension of cybercrime: Report from a trip to Ramnicu Valcea (Romania),” in *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany, Volume III*, U. Tottel, G. Bulanova-Hristova, and G. Flach, Eds. Bundeskriminalamt Criminalistic Institute, 2015, pp. 163–172.

[540] Digital Shadows Analyst Team, "Deer.io: Your One-Stop Shop for Cybercrime," jul 2016. [Online]. Available: https://www.digitalshadows.com/blog-and-research/deer-io-your-one-stop-shop-for-cybercrime/

[541] E. T. Hall, *The Silent Language.* New York: Doubleday & Co., 1959.

[542] ——, *Beyond culture.* New York: Anchor Books, 1976.

[543] T. J. Holt, "Examining the Role of Technology in the Formation of Deviant Subcultures," *Social Science Computer Review*, vol. 28, no. 4, pp. 466–481, nov 2010. [Online]. Available: http://ssc.sagepub.com/cgi/doi/10.1177/0894439309351344

[544] A. Stolerman, A. C. Islam, and R. Greenstadt, "From Language to Family and Back: Native Language and Language Family Identification from English Text," in *Proceedings of the NAACL HLT 2013 Student Research Workshop*, Atlanta, GA, 2013, pp. 32–39. [Online]. Available: http://www.aclweb.org/anthology/N13-2005

[545] S. Pontiroli and J. van der Wiel, "Coinvault, are we reaching the end of the nightmare?" sep 2015. [Online]. Available: https://securelist.com/coinvault-are-we-reaching-the-end-of-the-nightmare/72187/

[546] R. Shuter, "Intercultural New Media Studies: The Next Frontier in Intercultural Communication," *Journal of Intercultural Communication Research*, vol. 41, no. 3, pp. 219–237, 2012.

[547] M. Schulte, "The Language of the Underworld and its Sociolinguistic Significance," *Contributions to the Study of Language, Literature and Culture. Arbeitsblätter des Anglistischen Seminars Heidelberg*, vol. 1, pp. 45–60, 2010.

[548] B. Krebs, "Cultural CAPTCHAs," sep 2011. [Online]. Available: https://krebsonsecurity.com/2011/09/cultural-captchas/

[549] J. Matusitz, "The Role of Intercultural Communication in Cyberterrorism," *Journal of Human Behavior in the Social Environment*, vol. 24, no. 7, pp. 775–790, sep 2014. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/10911359.2013.876375?journalCode=whum20

[550] B. G. Westlake and M. Bouchard, "Criminal Careers in Cyberspace: Examining Website Failure within Child Exploitation Networks," *Justice Quarterly*, vol. 33, no. 7, pp. 1154–1181, nov 2016. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/07418825.2015.1046393

[551] B. Krebs, "When Undercover Credit Card Buys Go Bad," dec 2015. [Online]. Available: https://krebsonsecurity.com/2015/12/when-undercover-credit-card-buys-go-bad/

[552] A. Cafiero Giusti, “Banks Have a Harder Time Blending Among Fraudsters,” nov 2015. [Online]. Available: https://www.paymentssource.com/news/banks-have-a-harder-time-blending-among-fraudsters

[553] A. Acquisti, “Nudging privacy: The behavioral economics of personal information,” *Security & Privacy Economics*, vol. 7, no. 6, pp. 72–75, 2009. [Online]. Available: http://ieeexplore.ieee.org/document/5370707/

[554] D. Maurer, “The Argot of Confidence Men,” *American Speech*, vol. 15, no. 2, pp. 113–123, apr 1940. [Online]. Available: http://www.jstor.org/stable/486816?origin=crossref

[555] B. D. Johnson, F. Bardhi, S. J. Sifaneck, and E. Dunlap, “Marijuana Argot As Subculture Threads: Social Constructions by Users in New York City,” *British Journal of Criminology*, vol. 46, no. 1, pp. 46–77, apr 2005. [Online]. Available: http://bjc.oxfordjournals.org/cgi/doi/10.1093/bjc/azi053

[556] R. Navigli, “Word Sense Disambiguation: A Survey,” *ACM Computing Surveys*, vol. 41, no. 2, pp. 1–69, feb 2009. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1459352.1459355

[557] A. Pabst, “Euro-Atlantic and Eurasian Security in a Multipolar World,” *American Foreign Policy Interests*, vol. 33, no. 1, pp. 26–40, 2011. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/10803920.2011.552036

[558] R. Peerenboom, “The Future of Law in a Multipolar World: Toward a Global New Deal.” [Online]. Available: https://ssrn.com/abstract=1846263

[559] D. Drissel, “Internet Governance in a Multipolar World: Challenging American Hegemony,” *Cambridge Review of International Affairs*, vol. 19, no. 1, pp. 105–120, 2006. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/09557570500501812

[560] A. Bendiek, “Why We Need a Transatlantic Deal on Cyber Security and Privacy,” sep 2013. [Online]. Available: http://www.gmfus.org/blog/2013/09/09/why-we-need-transatlantic-deal-cyber-security-and-privacy

[561] E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom.* Ingram Publisher Services, 2012.

[562] TASS, “Foreign Ministry: Western media plan to accuse Russia of hacking Olympic media resources,” feb 2018. [Online]. Available: http://tass.com/politics/988952

[563] E. Nakashima and J. Gillum, “U.S. moves to ban Kaspersky software in federal agencies amid concerns of Russian espionage,” sep 2017. [Online]. Available: https://www.washingtonpost.com/world/national-

security/us-to-ban-use-of-kaspersky-software-in-federal-agencies-amid-concerns-of-russian-espionage/2017/09/13/36b717d0-989e-11e7-82e4-f1076f6d6152{_}story.html?utm{_}term=.170267354c44

[564] Ministry of Foreign Affairs, "'Building Digital Bridges'. International Cyber Strategy. Towards an integrated international cyber policy," 2017. [Online]. Available: https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

[565] J. Zittrain, "Law and technology: The end of the generative internet," *Communications of the ACM*, vol. 52, no. 1, pp. 18–20, 2009. [Online]. Available: https://cacm.acm.org/magazines/2009/1/15660-law-and-technology-the-end-of-the-generative-internet/abstract

[566] J. Healey, "Beyond Attribution: Seeking National Responsibility in Cyberspace," Atlantic Counsel, Tech. Rep., 2012. [Online]. Available: http://www.atlanticcouncil.org/publications/issue-briefs/beyond-attribution-seeking-national-responsibility-in-cyberspace

[567] J. Lytvynenko and K. Collier, "Another Russian Hacker Claims He's The One Who Hacked The DNC," dec 2017. [Online]. Available: https://www.buzzfeed.com/janelytvynenko/russian-hacker-dnc-confession?utm{_}term=.hsJAOm053{#}.yjn8gXNMR

[568] The Moscow Times, "Arrested Kaspersky Labs Cybercrimes Chief Says Russia Trades Hackers Immunity for Stolen Info," apr 2017. [Online]. Available: https://themoscowtimes.com/news/arrested-kaspersky-labs-cybercrimes-chief-says-russia-trades-hackers-immunity-for-stolen-info-57706

[569] A. Tselikov, "The Tightening Web of Russian Internet Regulation," nov 2014. [Online]. Available: http://cyber.law.harvard.edu/publications/2014/runet{_}regulation

[570] A. Soldatov and I. Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.* The Perseus Books Group, 2015.

[571] S. Caltagirone, A. Pendergast, and C. Betz, "The Diamond Model of Intrusion Analysis," The Center for Cyber Intelligence Analysis and Threat Research, Hanover, MD, Tech. Rep., 2013. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

[572] S. W. Brenner and J. J. . Schwerha IV, "Cybercrime Havens. Challenges and Solutions," *Business Law Today*, vol. 17, no. 2, pp. 49–52, 2007.

[573] K. Geers, *Strategic Cyber Security.* NATO CCD COE Publications, 2011.

[574] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime," *International Journal of Cyber Criminology*, vol. 8, no. 1, pp. 1–20, 2014.

[575] K. S. Williams, "Transnational developments in Internet law," in *Handbook of Internet Crime*, Y. Jewkes and M. Yar, Eds. Willan Publishing, 2010, ch. 22, pp. 466–491.

[576] T. Holz, C. Gorecki, K. Rieck, and F. C. Freiling, "Measuring and Detecting Fast-Flux Service Networks," in *MALWARE 2008. 3rd International Conference on Malicious and Unwanted Software*, 2008, pp. 24 – 31.

[577] Trend Micro, "Turning the Tables on Cyber Attacks. Responding to Evolving Tactics," Trend Micro, Tech. Rep., 2014. [Online]. Available: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf

[578] RedSocks, "Windows Malware Annual Report 2014 And Prognosis 2015," RedSocks, Tech. Rep., 2015. [Online]. Available: http://pronovus.nl/documenten/2014{_}redsocks{_}malware{_}trends{_}annual{_}report{_}20150223-final.pdf

[579] McAfee, "McAfee Labs Threats Report March 2016," Intel Security, Tech. Rep., 2016. [Online]. Available: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

[580] GReAT, "Lazarus Under The Hood," apr 2017. [Online]. Available: https://securelist.com/lazarus-under-the-hood/77908/

[581] A. Kigerl, "Routine Activity Theory and the Determinants of High Cybercrime Countries," *Social Science Computer Review*, vol. 30, no. 4, pp. 470–486, nov 2012. [Online]. Available: http://ssc.sagepub.com/cgi/doi/10.1177/0894439311422689

[582] ——, "Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates," *International Journal of Cyber Criminology*, vol. 10, no. 2, pp. 147–169, 2016.

[583] W. Shim, L. Allodi, and F. Massacci, "Crime pays if you are just an average hacker," in *Proceedings of the 2012 ASE International Conference on Cyber Security*. Alexandria, VA: IEEE, 2012, pp. 62–68. [Online]. Available: http://ieeexplore.ieee.org/document/6542527/

[584] R. van Heur, "Fears of software skills shortage in Germany and the Netherlands," jan 2016. [Online]. Available: http://www.computerweekly.com/news/4500269840/Fears-of-software-skills-shortage-in-Germany-and-the-Netherlands

[585] J. Witteveen, "My Smart Industry. Slimmer groeien, sneller groeien," ING Economisch Bureau, Tech. Rep., 2017. [Online]. Available: https://www.ing.nl/media/ING{_}EBZ{_}my-smart-industry{_}tcm162-135030.pdf

[586] Council of Europe, "Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime. Status as of 04/05/2018," 2018. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p{_}auth=0NEZLR7g

[587] Redactie, "15-jarige Robin W. uit Ruurlo 'leider' bij DDoS-aanval op Ziggo," oct 2015. [Online]. Available: https://www.tubantia.nl/achterhoek/15-jarige-robin-w-uit-ruurlo-leider-bij-ddos-aanval-op-ziggo{~}a330117c/

[588] C. Ahlberg, "Chasing Foxes by the Numbers: Patterns of Life and Activity in Hacker Forums," in *Blackhat Europe 2016*, London, UK, 2016. [Online]. Available: https://www.blackhat.com/eu-16/briefings/schedule/{#}chasing-foxes-by-the-numbers-patterns-of-life-and-activity-in-hacker-forums-4881

[589] R. Fournier and M. Latapy, "Temporal Patterns of Pedophile Activity in a P2P Network: First Insights about User Profiles from Big Data," *International Journal of Internet Science*, vol. 10, no. 1, pp. 8–19, 2015.

[590] Europol, "An Introduction to Bitcoin Mixers," 2018.

[591] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in *2015 IFIP/IEEE International Symposium on Integrated Network Management*. IEEE, 2015, pp. 243–251. [Online]. Available: http://ieeexplore.ieee.org/document/7140298/

[592] W. Chang, A. Wang, A. Mohaisen, S. Chen, W. Chang, A. Wang, A. Mohaisen, and S. Chen, "Characterizing botnets-as-a-service," in *Proceedings of the 2014 ACM conference on SIGCOMM*, vol. 44, no. 4. New York, New York, USA: ACM Press, 2014, pp. 585–586. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2619239.2631464

[593] Z. Berkay Celik and S. Oktug, "Detection of Fast-Flux Networks using various DNS feature sets," in *2013 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, jul 2013, pp. 000 868–000 873. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6755058

[594] N. Slepogin, "Dridex: a history of evolution," Kaspersky Lab, Tech. Rep., 2017. [Online]. Available: https://securelist.com/dridex-a-history-of-evolution/78531/

[595] S. Hongladarom, “Personal Identity and the Self in the Online and Offline World,” *Minds and Machines*, vol. 21, no. 4, pp. 533–548, nov 2011. [Online]. Available: http://link.springer.com/10.1007/s11023-011-9255-x

[596] L. Sade-Beck, “Internet Ethnography: Online and Offline,” *International Journal of Qualitative Methods*, vol. 3, no. 2, pp. 45–51, jun 2004. [Online]. Available: http://journals.sagepub.com/doi/10.1177/160940690400300204

[597] E. van der Veen, “Automotive,” *Blauw*, vol. 14, no. 3, pp. 36–37, 2018.

[598] J. Aldridge and R. Askew, “Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement.” *The International journal on drug policy*, vol. 41, pp. 101–109, mar 2017. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/28089207

[599] Europol, “European Union Serious and Organised Crime Threat Assessment 2017. Crime in the age of technology,” European Union, Tech. Rep., 2017. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

[600] Rb. Zeeland-West-Brabant, “ECLI:NL:RBZWB:2016:3877,” jun 2016. [Online]. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2016:3877

[601] R. Atlas, “"Offensible Space" - Law and Order Obstruction through Environmental Design,” *Proceedings of the Human Factors and Ergonomics Society. 34th Annual Meeting*, vol. 34, no. 7, pp. 570–574, 1990. [Online]. Available: http://journals.sagepub.com/doi/abs/10.1177/154193129003400708

[602] ——, “The other side of CPTED,” *Security Management*, vol. 35, no. 3, pp. 63–67, 1991. [Online]. Available: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=143812

[603] B. Krebs, “The World Has No Room For Cowards,” 2013. [Online]. Available: https://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/

[604] ——, “Mail from the (Velvet) Cybercrime Underground,” 2013. [Online]. Available: https://krebsonsecurity.com/2013/07/mail-from-the-velvet-cybercrime-underground/

[605] C. Dawson, “An Orthodox Holiday For Some Unorthodox Actors,” jan 2016. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/An-Orthodox-Holiday-For-Some-Unorthodox-Actors

[606] J. Mathiason, M. Mueller, H. Klein, M. Holitscher, and L. McKnight, “Internet Governance: The State of Play,” The Internet Governance Project, Tech. Rep., 2004. [Online]. Available: https://www.internetgovernance.org/wp-content/uploads/mainreport-final.pdf

[607] L. Lessig, “The Law of the Horse: What Cyberlaw Might Teach,” *Harvard Law Review*, vol. 113, pp. 501–549, 1999.

[608] C. Raab and P. de Hert, “The regulation of technology: policy tools and policy actors,” 2007. [Online]. Available: http://ssrn.com/abstract=1030263

[609] ——, “Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood,” in *Regulating Technologies*, R. Brownsword and K. Yeung, Eds. Hart Publishing, 2008, ch. 12, pp. 263–285.

[610] National Cyber Security Centre, “National Cyber Security Strategy 2. From awareness to capability,” Ministry of Security and Justice, Tech. Rep., 2013.

[611] D. Broeders, *The public Core of the Internet. An international agenda for Internet governance.* Amsterdam: Amsterdam University Press, jan 2015. [Online]. Available: https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

[612] M. S. Nuth, “Taking advantage of new technologies: For and against crime,” *Computer Law and Security Report*, vol. 24, no. 5, pp. 437–446, 2008.

[613] G. King and C. Murray, “Rethinking Human Security,” *Political Science Quarterly*, vol. 116, no. 4, pp. 585–610, 2001. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.2307/798222/abstract

[614] Study Group on Europe’s Security Capabilities, “A Human Security Doctrine for Europe: Report of the Barcelona Study Group on Europe’s Security Capabilities,” Barcelona, Tech. Rep., 2003. [Online]. Available: http://www.lse.ac.uk/Depts/global/Publications/HumanSecurityDoc-trine.pdf;

[615] R. Paris, “Human Security. Paradigm Shift or Hot Air?” *International Security*, vol. 26, no. 2, pp. 87–102, 2001.

[616] BBC News, “Dutch government says no to ’encryption backdoors’,” jan 2016. [Online]. Available: https://www.bbc.com/news/technology-35251429

[617] M. de Bruijne, “Hack_Right | Strafblad voorkomen,” 2018. [Online]. Available: https://www.opportuun.nl/edities/2018/02/hackright

[618] K. A. Annan, “Towards a Culture of Peace: Letters to Future Generations,” United Nations, Tech. Rep., 2005. [Online]. Available: http://unesdoc.unesco.org/images/0011/001185/118573e.pdf

[619] B.-J. Koops, “Criminal Law and Cyberspace as a Challenge for Legal Research,” *ScriptEd*, vol. 9, no. 3, pp. 354–366, 2012.

[620] U. Beck, “The Terrorist Threat: World Risk Society Revisited,” *Theory, Culture & Society*, vol. 19, no. 4, pp. 39–55, aug 2002. [Online]. Available: http://tcs.sagepub.com/cgi/doi/10.1177/0263276402019004003

[621] Q. Eijkman, “Police Technology and Human Rights: A quest for accountability.” in *Technological Led Policing*, P. Pauw, E., de, Ponsaers, P., Vijver, K., van der, Bruggeman, W., Deelman, Ed. Antwerpen/Apeldoorn: Maklu, 2012, ch. 9.

[622] A. Irons and H. Lallie, “Digital Forensics to Intelligent Forensics,” *Future Internet*, vol. 6, no. 3, pp. 584–596, sep 2014. [Online]. Available: http://www.mdpi.com/1999-5903/6/3/584

[623] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the age of sophisticated cyber attacks,” *Computers & Security*, vol. 72, pp. 212–233, jan 2018. [Online]. Available: https://www-sciencedirect-com.bris.idm.oclc.org/science/article/pii/S0167404817301839

[624] B.-J. Koops, “The trouble with European data protection law,” *International Data Privacy Law*, vol. 4, no. 4, pp. 250–261, nov 2014. [Online]. Available: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipu023

[625] N. Diakopoulos, “Accountability in algorithmic decision making,” *Communications of the ACM*, vol. 59, no. 2, pp. 56–62, jan 2016. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2886013.2844110

[626] D. Broeders, E. Schrijvers, and E. Hirsch Ballin, “Big Data and Security Policies: Serving Security, Protecting Freedom,” 2017.

[627] Rb. Amsterdam, “ECLI:NL:RBAMS:2018:2504,” 2018. [Online]. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:2504

[628] T. Pöysti, “ICT and Legal Principles: Sources and Paradigm of Information Law,” *Scandinavian studies in law*, vol. 47, pp. 559–600, 2004.

[629] S. Ó. Ciardhuáin, “An Extended Model of Cybercrime Investigations,” *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.1289{&}rep=rep1{&}type=pdf

[630] S. Laville, "Anonymous hacks into phone call between FBI and Scotland Yard," feb 2012. [Online]. Available: https://www.theguardian.com/technology/2012/feb/03/anonymous-hacks-call-fbi-scotland-yard

[631] R. Anderson, R. Bohme, R. Clayton, and T. Moore, "Security Economics and The Internal Market," European Network and Information Security Agency, Tech. Rep., 2008. [Online]. Available: https://www.enisa.europa.eu/publications/archive/economics-sec/at{_}download/fullReport

[632] Europol, "The Internet Organised Crime Threat Assessment (iOCTA)," Europol, Tech. Rep., 2014. [Online]. Available: https://www.europol.europa.eu

[633] F. M. Pinguelo, W. Lee, and B. W. Muller, "Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow," *Virginia Journal of Law & Technology*, vol. 17, no. 1, pp. 76–88, 2012.

[634] L. Johnston and C. Shearing, *Governing Security: Explorations in Policing and Justice.* London: Routledge, 2003.

[635] L. Huey, J. Nhan, and R. Broll, "'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime," *Criminology and Criminal Justice*, vol. 13, no. 1, pp. 81–97, jun 2012. [Online]. Available: http://crj.sagepub.com/content/13/1/81

[636] R. Wettenhall, "The rhetoric and reality of public-private partnerships," *Public organization review*, vol. 3, no. 1, pp. pp.77–107, 2003.

[637] A. Mell, "Promoting Market Failure: Fighting Crime with Asymmetric Information," 2015. [Online]. Available: https://docs.google.com/viewer?a=v{&}pid=sites{&}srcid=ZGVmYXVsdGRvbWFpbnxhbWVsbGVjb258Z3g6NWYyMTE1YjI1NzdlNjFmMQ

[638] I. Ladegaard, "We Know Where You Are, What You Are Doing and We Will Catch You," *The British Journal of Criminology*, vol. 58, no. 2, pp. 414–433, feb 2018. [Online]. Available: https://academic.oup.com/bjc/article/58/2/414/3760066

[639] S. L. Hal, "Intelligence Sharing With Russia: A Practitioner's Perspective - Carnegie Endowment for International Peace," 2017. [Online]. Available: http://carnegieendowment.org/2017/02/09/intelligence-sharing-with-russia-practitioner-s-perspective-pub-67962

[640] H. Modderkolk and T. Kreling, "Dutch police works together with Russia's FSB, despite political tensions," 2017. [Online]. Available: https://www.volkskrant.nl/tech/dutch-police-works-together-with-russia-s-fsb-despite-political-tensions{~}a4497360/

[641] R. Anderson, "Privacy versus government surveillance: where network effects meet public choice," in *13th Annual Workshop on the Economics of Information Security*, State College, PA, 2014. [Online]. Available: http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf

[642] V. Mavroeidis and S. Bromander, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence," in *2017 European Intelligence and Security Informatics Conference (EISIC)*. Athens, Greece: IEEE, sep 2017, pp. 91–98. [Online]. Available: http://ieeexplore.ieee.org/document/8240774/

[643] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security - WISCS '14*. New York, New York, USA: ACM Press, 2014, pp. 51–60. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2663876.2663883

[644] D. Bigo, "International Political Sociology," in *Security Studies. An Introduction.*, P. D. Williams, Ed. Oxon and New York: Routledge, 2008, pp. 116–129.

[645] S. Ransbotham and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, vol. 20, no. 1, pp. 121–139, 2009. [Online]. Available: http://www.jstor.org.bris.idm.oclc.org/stable/23015464

[646] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, mar 1983. [Online]. Available: http://ieeexplore.ieee.org/document/1056650/

[647] Mandiant, "M-Trends 2017. A view from the front lines," Mandiant, a FireEye company, Tech. Rep., 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html

[648] GReAT Computer Incidents Investigation Department, "APT-style bank robberies increase with Metel, GCMAN and Carbanak 2.0 attacks," 2016. [Online]. Available: https://securelist.com/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/73638/

[649] Crime Russia, "Hackers of Russian group Cobalt attacked 250 companies around the world," aug 2017. [Online]. Available: https://en.crimerussia.com/gromkie-dela/hackers-of-russian-group-cobalt-attacked-250-companies-around-the-world/

[650] C. Cimpanu, "UK Police Arrest Suspect Behind Mirai Malware Attacks on Deutsche Telekom," 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/uk-police-arrest-suspect-behind-mirai-malware-attacks-on-deutsche-telekom/

[651] M. Casayuran, "CUTWAIL Spambot Leads to UPATRE-DYRE Infection," oct 2014. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/cutwail-spambot-leads-to-upatre-dyre-infection/

[652] Trend Micro, "SIMDA: A Botnet Takedown," apr 2015. [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/

[653] Kaspersky Lab US, "Angler by Lurk: Why the infamous cybercriminal group that stole millions was renting out its most powerful tool," 2016. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2016{_}angler-by-lurk-why-the-infamous-cybercriminal-group-that-stole-millions-was-renting-out-its-most-powerful-tool

[654] B. Krebs, "Three Charged in Connection with 'Gozi' Trojan," jan 2013. [Online]. Available: https://krebsonsecurity.com/2013/01/three-men-charged-in-connection-with-gozi-trojan/{#}more-6878

[655] T. G., "Hacking as a Service: How Much Does it Cost to Hack an Account?" apr 2014. [Online]. Available: https://www.symantec.com/connect/blogs/hacking-service-how-much-does-it-cost-hack-account

[656] SecurityWeek News, "Wildfire Ransomware Operators Made $80,000 in One Month," aug 2016. [Online]. Available: https://www.securityweek.com/wildfire-ransomware-operators-made-80000-one-month

[657] B. Brenner, "5 ransomware as a service (RaaS) kits," dec 2017. [Online]. Available: https://nakedsecurity.sophos.com/2017/12/13/5-ransomware-as-a-service-raas-kits-sophoslabs-investigates/

[658] P. Paganini, "Ennetcom - Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case," 2017. [Online]. Available: http://securityaffairs.co/wordpress/57036/cyber-crime/blackberry-pgp-messages.html

[659] NOS, "Miljoen cash gevonden bij onderzoek naar crypto-gsm's," 2017. [Online]. Available: https://nos.nl/artikel/2172299-miljoen-cash-gevonden-bij-onderzoek-naar-crypto-gsm-s.html

[660] S. Gibbs and L. Beckett, "Dark web marketplaces AlphaBay and Hansa shut down," 2017. [Online]. Available: https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down

[661] Federal Bureau of Investigation, "Three Alleged International Cyber Criminals Responsible for Creating and Distributing Virus That Infected Over One Million Computers and Caused Tens of Millions of Dollars

in Losses Charged in Manhattan Federal Court," 2013. [Online]. Available: https://archives.fbi.gov/archives/newyork/press-releases/2013/three-alleged-international-cyber-criminals-responsible-for-creating-and-distributing-virus-that-infected-over-one-million-computers-and-caused-tens-of-millions-of-dollars-in-losses-charged-in-

[662] C. Cimpanu, "Police Seize Servers of Bulletproof Provider Known For Hosting Malware Ops," may 2018. [Online]. Available: https://www.bleepingcomputer.com/news/security/police-seize-servers-of-bulletproof-provider-known-for-hosting-malware-ops/

[663] Europol, "International operation targets customers of counter anti-virus and crypter services: 6 arrested and 36 interviewed," 2017. [Online]. Available: https://www.europol.europa.eu/newsroom/news/international-operation-targets-customers-of-counter-anti-virus-and-crypter-services-6-arrested-and-36-interviewed

[664] P. Vugts, "Recherche doet inval in spyshop aan Postjesweg," 2015. [Online]. Available: http://www.ad.nl/amsterdam/recherche-doet-inval-in-spyshop-aan-postjesweg{~}ae8e1d04/

[665] M. van Wely, "Witwasreus Bitcoins opgepakt," 2016. [Online]. Available: http://www.telegraaf.nl/binnenland/25420312/{_}{_}Witwasreus{_}Bitcoins{_}opgepakt{_}{_}.html

[666] A. Mundo, J. Fokker, and T. Roccia, "Rapidly Evolving Ransomware GandCrab Version 5 Partners With Crypter Service for Obfuscation," oct 2018. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/rapidly-evolving-ransomware-gandcrab-version-5-partners-with-crypter-service-for-obfuscation/

[667] US-CERT, "Avalanche (crimeware-as-a-service infrastructure)," dec 2016. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-336A

[668] A. Greenberg, "How Dutch Police Took Over Hansa, a Top Dark Web Market," mar 2018. [Online]. Available: https://www.wired.com/story/hansa-dutch-police-sting-operation/

[669] R. Holland, R. Amado, and M. Marriott, "Seize and Desist? The State of Cybercrime in the Post-AlphaBay and Hansa Age," Digital Shadows, Tech. Rep., 2018.

[670] R. Schoemaker, "Politie over de schreef bij botnetontmanteling - UPDATE," oct 2010. [Online]. Available: http://webwereld.nl/security/45513-politie-over-de-schreef-bij-botnetontmanteling---update

[671] D. van der Kroft, "Bredolab: Trojaans paradepaardje van het KLPD?" nov 2011. [Online]. Available: https://www.bof.nl/2011/11/07/bredolab-trojaans-parade-paardje-van-het-klpd/

[672] A. Hutchings and T. J. Holt, "The online stolen data market: disruption and intervention approaches," *Global Crime*, vol. 18, no. 1, pp. 11–30, 2017.

[673] N. J. Healey, O. Angelopoulou, and D. Evans, "A Discussion on the Recovery of Data from a Virtual Machine," in *2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*. Xi'an, China: IEEE, sep 2013, pp. 603–606. [Online]. Available: http://ieeexplore.ieee.org/document/6631686/

[674] D. O'Reilly, "Analysis of the Crime Attribution Characteristics of Various IPv6 Address Assignment Techniques," Internet Engineering Task Force, Tech. Rep., 2018. [Online]. Available: https://tools.ietf.org/id/draft-daveor-ipv6-crime-attribution-00.html

[675] K. Bojarski, "Dealer, Hacker, Lawyer, Spy. Modern Techniques and Legal Boundaries of Counter-cybercrime Operations," *The European Review of Organised Crime*, vol. 2, no. 2, pp. 25–50, 2015.

[676] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things Forensics: Challenges and Approaches," in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*. Austin, TX: ICST, 2013. [Online]. Available: http://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254159

[677] Centraal Bureau voor de Statistiek, "Afname criminaliteit in alle delen Nederland," mar 2018. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2018/09/afname-criminaliteit-in-alle-delen-nederland

[678] J. Fokker, "Organizations Leave Backdoors Open to Cheap Remote Desktop Protocol Attacks," jul 2018. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/organizations-leave-backdoors-open-to-cheap-remote-desktop-protocol-attacks/