RESEARCH AGENDA

THE HUMAN FACTOR IN CYBERCRIME AND CYBERSECURITY

eleven
international publishing

With the digitization of society, crime has also digitized. Digitization has consequences for the entire spectrum of crime and raises all sorts of questions. For example, are we dealing with a new type of offender, or with the same old offenders who simply moved their activities online? How can potential victims be made resilient against attacks? And who should protect potential victims: the police, commercial cybersecurity companies, or internet service providers?

To date, many of these questions remain unanswered. This is partly because current studies have a strong focus on technology or are exploratory in nature, suffer from methodological limitations and focus on just a few of the many types of cybercrime.

The aim of this research agenda is to stimulate research on the human factor in cybercrime and cybersecurity. The agenda provides the state-of-the-art of research on the role of the human factor in this field. In addition, examples are given of important research questions and innovative methods and datasets that are needed for future studies. This agenda can be seen as a foundation for further thought with disciplines, inside and outside the social sciences, about how these topics and questions can best be answered.

ISBN 978-94-6236-753-1

RESEARCH AGENDA THE HUMAN FACTOR
IN CYBERCRIME AND CYBERSECURITY

RESEARCH AGENDA THE HUMAN FACTOR IN CYBERCRIME AND CYBERSECURITY

Rutger Leukfeldt (editor)

eleven
international publishing

Published, sold and distributed by Eleven International Publishing
P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
e-mail: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada
International Specialized Book Services
920 NE 58th Avenue, Suite 300
Portland, OR 97213-3786, USA
Tel.: 1-800-944-6190 (toll-free)
Fax: +1-503-280-8832
orders@isbs.com
www.isbs.com

Eleven International Publishing is an imprint of Boom uitgevers Den Haag.

This research agenda is the outcome of the national cybercrime initiative ('NASA Cybercrime') coordinated by the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and funded by the Netherlands Organization for Scientific Research (NWO).

ISBN 978-94-6236-753-1
ISBN 978-94-6274-706-7 (E-book)

Printed in The Netherlands

CONTENTS

PREFACE

CYBER AND OTHER SPACE RESEARCH: THE BIGGER PICTURE

Space research in antiquity can be characterized as mono-disciplinary research: astronomers in Mesopotamia observed and recorded the position, brightness and movement of the sun, moon, planets and stars. Their field of vision was heavenly and they recorded everything down on earth on clay tablets. Thanks to applications of IT research we can now peruse the work of researchers from that time. Nowadays, there are many freeware planetarium programs, sky maps and astrology apps in circulation, which you can use to reproduce and view a starry sky 33 AD. The field of vision of modern astronomers is considerably broader than that of their ancestors. Space research nowadays is impossible without IT research.

Cyberspace research actually began under the name information security, as a mono-disciplinary direction within IT. Meanwhile, the field of vision of the cybersecurity research community greatly expanded into the darkest ends of the world-wide web. This research is not possible without the contributions of the humanities and social sciences. Criminologists, lawyers, economists and ethicists can make an outstanding contribution to the broad spectrum of cybersecurity research.

The cybersecurity research community is justifiably increasing its attention to the human factor and the socio-technical side, such as social engineering. The Dutch Cybersecurity Platform for Higher Education and Research – dcypher – a public-private agenda-setting platform, is committed to connecting the brand new NWO domains of Sciences (ENW),

Applied and Engineering Sciences (TTW) and Social Sciences and Humanities (SGW) in the area of cybersecurity research to one another. In the past several calls for cybersecurity research proposals were organized and funded by various NWO science departments. As a framework for these calls, successive editions of the multidisciplinary domain – and top sector crosscutting National Cyber Security Research Agenda (NCSRA) were used.

The research agenda "*The Human Factor in Cybercrime and Cybersecurity*" deserves to be executed. The team of authors preparing a new edition of the NCSRA, under coordination of dcypher, will definitely use this agenda as input. In particular, Chapter 8 provides attractive challenges. Field consultations for the NCSRA III will take place at the end of 2017. I wholeheartedly welcome the participation of all human factor researchers who contributed to this agenda, and to a valuable broadening of cyberspace research.

Jan Piet Barthel
Director dcypher
www.dcypher.nl

INTRODUCTION

Rutger Leukfeldt

Digitized society

Our society is highly digitized. On a typical day, people use various information technology (IT) applications. The Netherlands is at the top of many lists related to IT use. The majority of the Dutch population, for example, has access to the internet (89% of households in 2015) and uses it every day in one way or another. IT is no longer solely used to communicate or to find information. In 2015, three quarters of the Dutch population was active on a social network, 77 percent used online banking and 10.1 million individuals shopped online (CBS, 2016). Furthermore, in 2015, virtually all companies had a broadband internet connection, 90 percent had their own website, 74 percent provided their staff with laptops, tablets or smartphones, and 28 percent used cloud services to store information. Finally, the Netherlands plays an important role in the infrastructure of the internet. In December 2015, an important internet exchange hub, the Amsterdam Internet Exchange (AMS-IX) processed 864 thousand terabytes of data traffic (CBS, 2016).

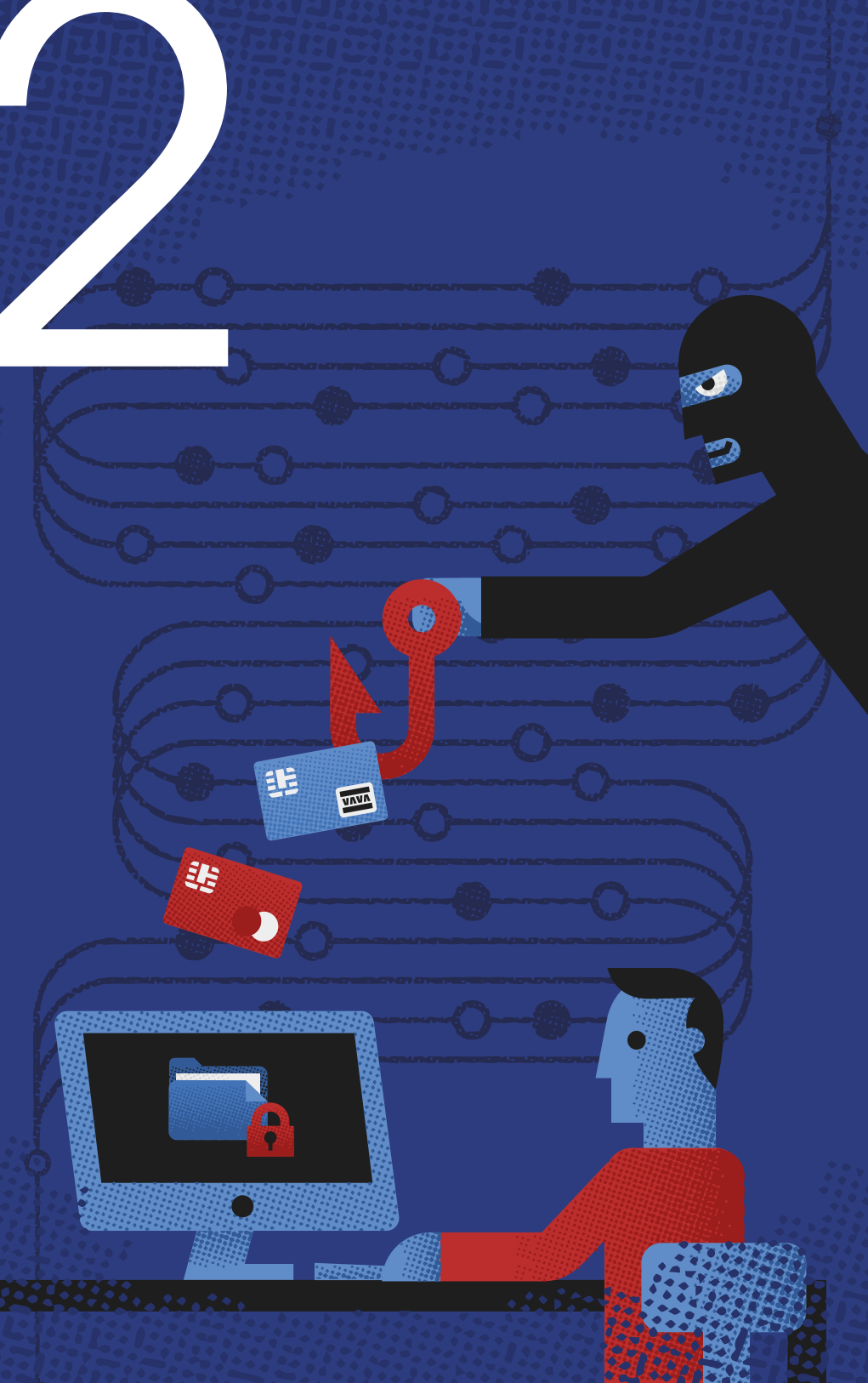
Digitization and crime

With the digitization of society, crime has also digitized. On the one hand, there are new offenses, such as hacking databases and taking down websites or networks. On the other hand, there are traditional forms of crime in which IT plays an increasingly important role in its realization. Examples are internet fraud and cyberstalking. Digitization has consequences for the entire spectrum of crime and raises all sorts

of questions. For example, are we dealing with the same old offenders who have moved their activities online, or is there a new type of offender with the same characteristics and motives? Which personal and situational characteristics provide an increased or decreased risk of cybercrime victimization? And who should protect potential victims: the police, commercial cybersecurity companies, or internet service providers (ISPs) and hosting providers?

The human factor

The fact that digitization brings new risks is widely recognized. Thanks to funds for cybercrime and cybersecurity research, more and more scientific research is being conducted in this field. Examples include funding programs from NWO and SBIR (the Netherlands), EPSRC (United Kingdom), NordForsk (Nordic countries) and NSF (USA). These funding programs call for multidisciplinary research and emphasize that technical as well as human aspects are of interest. However, most of the studies conducted within these programs have a strong focus on technology, for example, on developing tools and techniques to detect or stop incidents. In order to stimulate non-technological research, the research agenda "The Human Factor in Cybercrime and Cybersecurity" has been developed. Research on the human factor in cybercrime and cybersecurity is necessary to take the step from stopping incidents to understanding and preventing incidents.



ABOUT THIS RESEARCH AGENDA

Rutger Leukfeldt

Goal

The aim of this research agenda is to stimulate research on the human factor in cybercrime and cybersecurity. The human factor in cybercrime and cybersecurity includes offenders, victims and actors who play a role in tackling crime. In this agenda, researchers in the field of non-technological research into cybercrime and cybersecurity jointly provide the state-of-the-art of research on the role of the human factor in this research field. In addition, examples are given of important research questions and innovative research methods and datasets that are needed for future research on the human factor in cybercrime and cybersecurity.

Human factor approach

For the development of this research agenda, experts in the field of non-technological research on cybercrime and cybersecurity have been the focus of consultations. This does not imply that technical sciences are not needed to answer the research questions outlined in this agenda. That different disciplines are needed to study and understand cybercrime and cybersecurity is not in doubt. This research agenda can be seen as a foundation for further thought with disciplines, inside and outside the social sciences, about how the formulated research topics and research questions can best be answered.

Organization

The Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) was the initiator of this research agenda. The NSCR worked closely with researchers associated with research groups from nine universities, four universities of applied sciences, and organizations such as the Scientific Research and Documentation Centre (WODC) of the Ministry of Security and Justice, Statistic Netherlands (CBS), TNO, the Dutch National Cyber Security Center (NCSC), the Dutch National Police, the Dutch Public Prosecution Service, the Dutch Probation Service and the Netherlands Council for the Judiciary. A total of 46 people from 26 organizations contributed to this research agenda (see Annex 1 and 2).

Methods

In total, 22 researchers and practitioners co-authored one or more of the three themes in this research agenda: offenders, victims and tackling crime. For each theme, these authors provided a state-of-the-art of research into the human factor in cybercrime and cybersecurity. In addition, important research topics and research question were identified. See Annex 1 for the list of authors. The results of this exercise were used as input for three discussion sessions. Forty-six people attended these sessions (see Annex 1 and Annex 2). During the discussion sessions, the results of the literature reviews were discussed (i.e., is this a good representation of the theme? Are these the most important topics within this theme?) Participants also discussed important research topics, relevant research questions and possibilities for the use of innovative data sources and research methods. Therefore, this research agenda is based on literature reviews as well as discussions with experts.


3

DEFINITIONS AND TOPICS

Rutger Leukfeldt

Definitions

Cybersecurity, cybercrime, e-crime, high-tech crime, digitized crime. There are many terms used to describe crimes or incidents in which IT is the target or where IT plays a major role in the realization of the offense. When it comes to criminological research into crime and IT, in general, two types of crimes are distinguished: "new" types of crimes that are aimed at IT and committed through the use of IT (e.g., hacking), and "traditional" crimes that are not focused on IT, but where IT is a substantial facilitating factor for committing the offense (e.g., fraud via the internet) (e.g., Holt & Bossler, 2014; McGuire & Dowling, 2013). Depending on the type of attack, cybersecurity incidents fall within one of these categories. In this research agenda, the term "cyber-dependent crimes" is used for those within the former category and "cyber-enabled crimes" for the latter category. "Cybercrime" is used as an umbrella term for both categories.

Various forms of cybercrime can be identified. Cyber-dependent crimes, for example, include crimes such as hacking, creating botnets, infecting computers with malware and crippling IT systems using DDoS attacks. Cyber-enabled crimes include various traditional crimes such as fraud, threats and stalking. Sometimes crimes fall within both categories. For example, hacking to steal sensitive information from a company in order to extort that company or the use of malware to intercept login credentials of users of online bank accounts in order to commit fraud with these bank accounts. Consequently,

when the term "cybercrime" is used in this research agenda, it could therefore be about different types of crimes. For future studies into cybercrime, it is important to recognize this and to take into account the different types of cybercrimes and the characteristics related to them. The motives – and, therefore, choices of offenders and opportunities for intervention related to motivations – are quite different, for example, for an individual hacker who hacks for recognition, for a script kiddie who typically uses tools created by others without overseeing the consequences of their actions, and for traditional organized crime groups which hire IT specialists to commit cyberattacks. However, to aid readability, the term cybercrime is used throughout this document.

Topics

This research agenda is divided into three themes: offenders (individuals and networks), victims and tackling cybercrime.

Offenders

When it comes to offenders, topics such as the characteristics of individual offenders, their criminal careers and the social and psychological processes that play a role in the development of offending, are of importance. Furthermore, with regard to criminal networks, opportunity structures, business models, the use of facilitators and the use of the dark web to purchase and sell criminal tools and services are relevant. Chapter 4 of this research agenda covers individual cybercrime offenders, while Chapter 5 zooms in on cybercriminal networks.

Victims

With respect to victims it is, for example, relevant to gain insight into how users can be made more resilient against cyber-attacks, which characteristics of victims and their behavior both on- and offline makes them more or less attractive to cybercriminals, and what the impact of cybercrime on victims and society is. Chapter 6 discusses this topic in depth.

Tackling cybercrime

All kinds of parties play a role in tackling cybercrime. Relevant questions here concern the role end users can play, the role and responsibilities parties such as ISPs and social media platforms have, and whether the police are able to perform their traditional role as capable guardians. Chapter 7 covers this topic.


4

INDIVIDUAL CYBER-CRIME OFFENDERS

Marleen Weulen Kranenbarg, André van der Laan,
Christianne de Poot, Maite Verhoeven,
Wytske van der Wagen, Gijs Weijters

Nature and extent

There is little insight into the nature and extent of cybercrime offending. Based on official criminal justice figures, it is estimated that less than 0.01 percent of young people in the Netherlands are cybercrime offenders. Estimates based on survey research range from 5 percent to 22 percent (Bossler & Burrus, 2011; Holt et al., 2010a; Van der Laan & Goudriaan, 2016; Zebel et al., 2013). Further, a study into the use of IT in traditional crimes shows that in 41 percent of fraud cases and 16 percent of threat cases, IT is used to commit these crimes (Montoya, Junger & Hartel, 2013). With the ongoing digitization of our society, it is to be expected that IT will play an important role in the commissioning of more and more traditional crimes.

The question is whether traditional data and methods, such as criminal justice figures and victim surveys, can be used to get a good picture of cybercrime offenders (Hargreaves & Prince, 2013; Holt & Bossler, 2016; Van der Laan & Goudriaan, 2016; Zebel et al., 2013). More advanced methods, like text mining and data mining, can be used to make better use of traditional sources, while online sources, for example, social media platforms or online forums, can also be used (see, for example, Van der Laan, Beerthuizen & Weijters, 2016).

There is no clear picture of the nature and extent of cybercrime offending. With the ongoing digitization, it is also important to gain insight into the importance of the digital component within different types of cyber-dependent crimes and cyber-enabled crimes. Further, research is needed into how offenders of different types of cybercrime can be measured in a reliable way. Can traditional methods like surveys and police records still be used, which changes are needed and what are the possibilities of new online data sources and advanced data collection methods?

Demographic characteristics

Are we dealing with a new type of offender, or with traditional offenders on new turf? There are some studies that suggest that cybercrime offenders have the same demographics as traditional offenders. Cybercriminals, for example, are more likely to be men (Bachmann & Corzine, 2010; Hollinger, 1993; Li, 2008; Randazzo et al., 2005, UNODC, 2013) and more likely to be young (UNODC, 2013; Yar, 2005). However, it has also been suggested that they differ in ethnicity (Bachmann & Corzine, 2010; Li, 2008; Rogers, 2001; Skinner & Fream, 1997), they may even be younger than traditional offenders (Leukfeldt & Stol, 2012), and that age is related to their degree of technical skills (Fotinger & Ziegler, 2004; Van der Laan & Goudriaan, 2016). Finally, suspects in Dutch internet fraud cases are more likely to have a Dutch nationality when compared to traditional fraud cases (respectively, 96% and 72%) (Montoya et al., 2013).

Studies into characteristics, such as socioeconomic status, marital status, education, income and intelligence, suggest that some types of cybercrime offenders have different characteristics than traditional offenders (Aransiola & Asindemade, 2011; Bachmann & Corzine, 2010; Chiesa et al., 2008; Fotinger & Ziegler, 2004; Holt et al., 2012; Leukfeldt et al., 2010; Leukfeldt & Stol, 2012; Moon et al., 2010; Randazzo et al., 2005;

Schell & Melnychuk, 2011; Turgeman-Goldschmidt, 2011a). Dietrich et al. (2016) show that cybercrime offenders are more likely to be higher educated than offenders of traditional crimes. However, the possibility of purchasing cybercriminal tools on forums enables a larger group of less educated offenders to go down the path of cybercrime (UNODC, 2013).

Overall, there is a lack of empirical research into the characteristics of cybercrime offenders. It is not known, for example, whether cybercriminals have different characteristics than traditional offenders, and it is not known if and how offender characteristics interact with the motives for and execution of certain cybercrimes. Research is needed into the characteristics of offenders engaged in various forms of cybercrime (cyber-dependent crimes as well as cyber-enabled crimes). Traditional methods such as offender interviews have hardly been used to gain more insight. In addition, criminal meeting places on the darkweb offer new opportunities to recruit a new type of respondent or to conduct observational research.

Personality, self-control and interaction effects

Low self-control seems to be related to cybercrime offending (Donner et al., 2014; Holt et al., 2012; Hu et al., 2013; Kerstens & Jansen, 2016; Marcum, et al., 2014; Moon et al., 2010, 2013). Interestingly, however, the more technical cybercrimes in particular require a lot of knowledge, patience and planning, which would indicate high self-control (Bachmann, 2010; Holt & Bossler, 2014; Holt & Kilger, 2008; Willison, 2006). Other psychological characteristics related to cybercrime offenders are high online disinhibition or moral disengagement (Kerstens & Jansen, 2016; Young et al., 2007), abnormal moral development (Gordon & Ma, 2003), narcissism (Woo, 2003) introversion (Schell & Melnychuk, 2011), being manipulative (Rogers, 2001; Rogers, Smoak, & Liu, 2006), autism (Harvey

et al., 2016), lack of empathy, anxiety and computer addiction (Schell & Melnychuk, 2011). These characteristics differ between types of cybercrime (Rogers et al., 2006; Seigfried & Treadway, 2014).

There is no systematic empirical research on the psychological characteristics of cybercrime offenders engaged in the various types of offenses (cyber-dependent crimes as well as cyber-enabled crimes). The studies that have been done have severe limitations and focus on a limited number of offenses. Therefore, we lack insight into psychological characteristics related to cybercrime offending.

Social learning, deviant friends

The influence of friends and social learning through friends is much studied for cybercrime. Generally, a relationship can be seen between deviant behavior of friends and one's own behavior (Hollinger, 1993; Hutchings & Clayton, 2016; Marcum et al., 2014; Morris, 2011; Rogers, 2001). However, this effect differs for various types of cybercrime and it is not entirely clear which elements of social learning are most effective (Holt, 2009; Holt et al., 2010; Morris & Blackburn, 2009; Skinner & Fream, 1997). Although many have argued that committing cybercrime is learned from friends, this has not been established. Knowledge can also be learned from unknown persons through the internet, for example, on forums or chat boxes (Chu et al., 2010; Holt & Kilger, 2008; Holt el al., 2012; Hutchings & Holt, 2015; Hutchings, 2014; Leukfeldt et al., 2017b; Skinner & Fream, 1997; Soudijn & Zegers, 2012). Criminal attitudes of friends – whether or not friends disapprove of delinquent behavior – are also of importance when it comes to cybercrime offending (Palesh, Saltzman & Koopman, 2004). The relation between the behavior of friends and one's own behavior can be a result of a selection process whereby people prefer to select friends who exhibit the same behavior. This has not yet been studied

for cybercrimes, presumably because longitudinal data is needed for this. Furthermore, it seems that both online and offline social contacts are of importance, but it is still unclear to what extent the effect of online and offline contacts varies (Holt, 2007; Holt & Bossler, 2014; Leukfeldt, Kleemans, & Stol, 2016).

Social contacts seem to be an important factor for committing cybercrimes. Therefore, social contacts and selection processes have to be studied in greater depth. The various types of cyber-dependent crimes and cyber-enabled crimes should be included. Ideally, this needs to be done objectively and based on longitudinal data. For example, by mapping entire networks at schools. As online ties seem to be just as important as offline ties, it is also important to identify the online network, for example, friends on social media or forums.

IT knowledge

IT knowledge is an important factor in the ability of a person to commit cybercrimes. Personality traits, such as self-control, can affect the extent to which someone is able learn the required skills. On the other hand, friends may assist in acquiring knowledge, and all sorts of ready-to-use tools and services can be found on forums (Holt et al., 2012; Leukfeldt et al., 2010; Odinot et al., 2016; Skibell, 2002; Sood & Enbody, 2013).

It is unclear how much knowledge is needed to commit the different types of cybercrime. More insight into the role of IT knowledge is required. For example, how and where do cyber criminals gain their IT knowledge? Furthermore, IT skills can be used both positively and negatively. How can you ensure that people who have these skills use them in a positive way? What are the differences between individuals who label themselves as "white hat" and as "black

hat" hackers? Are there differences in the knowledge level needed to commit the various types of cyber-dependent crimes and cyber-enabled crimes?

Routine activities

Cybercrime does not require offenders and victims to converge in time and space. Routine activities of offenders, however, might provide opportunities to commit cybercrimes. Although research on routine activities is mainly limited to the routines of victims, there are suggestions that particular online activities and victimization in the past are related to offending (Hu et al., 2013; Kerstens & Jansen, 2016; Morris, 2011). Examples include gaming (Blackburn et al., 2014; Hu et al., 2013) and spending time in online communities (Hutchings & Clayton, 2016). Further, the timing of cyber-attacks appears to be linked to routine activities of offenders and victims (Maimon et al., 2013). In addition, traditional protective routine activities, like work, might also provide an opportunity to commit cybercrime (Randazzo et al., 2005; Willison, 2006).

It is important to understand whether offenders of various forms of cyber-dependent crimes and cyber-enabled crimes consciously seek opportunities to commit crimes, or whether they more or less come across opportunities to commit cybercrime by chance during their daily activities.

Subculture

Is there a subculture in which committing cybercrimes is seen as normal? So-called hackers' accounts may provide insight into hackers from the perspective of the offenders themselves (see, for example, Dizon, 2016; Turgeman-Goldschmidt, 2008; Steinmetz, 2015). Dutch hackers, for example, only label hacking as illegal when the goal is financial gain (Van der Wagen et al., 2016). Hacking is mainly described as a hobby or as

experimenting with technology, but certainly not as willingly and knowingly committing a crime. Various studies show neutralization techniques used by cybercriminals: denial of responsibility, denial of injury (no harm is done as long as you do not delete anything), denial of the victim (there is no victim, just an enemy), condemnation of the condemners (reference to the "real" criminals of the digital world), appeal to higher loyalties (e.g., I want to keep learning), self-fulfillment (to do the impossible, even if someone else defines that as wrong) (Goode & Cruise, 2006; Hutchings & Clayton, 2016; Morris, 2011; Rogers, 1999; Turgeman-Goldschmidt, 2009, 2011).

Further research is needed into the moral perceptions and neutralization techniques of cybercriminals. Is there a subculture in which committing cybercrimes is seen as something normal? And how does this influence young people who are experimenting with technology? Are traditional criminological theories like Sutherland's differential association theory or Sykes and Matza's neutralization techniques applicable to the different types of cyber criminals?

Criminal careers

Insight into the characteristics of criminal careers of cybercriminals and the processes that lead them to start, continue or stop such behavior is needed to develop effective interventions. Traditional life course research focuses on the question of when and why people start and stop criminal behavior, often by looking at factors related to coming of age, such as getting a job, a house or marriage. Longitudinal studies are the most reliable way to study this. However, no such studies on criminal careers of cybercriminals exist (Holt & Bossler, 2014).

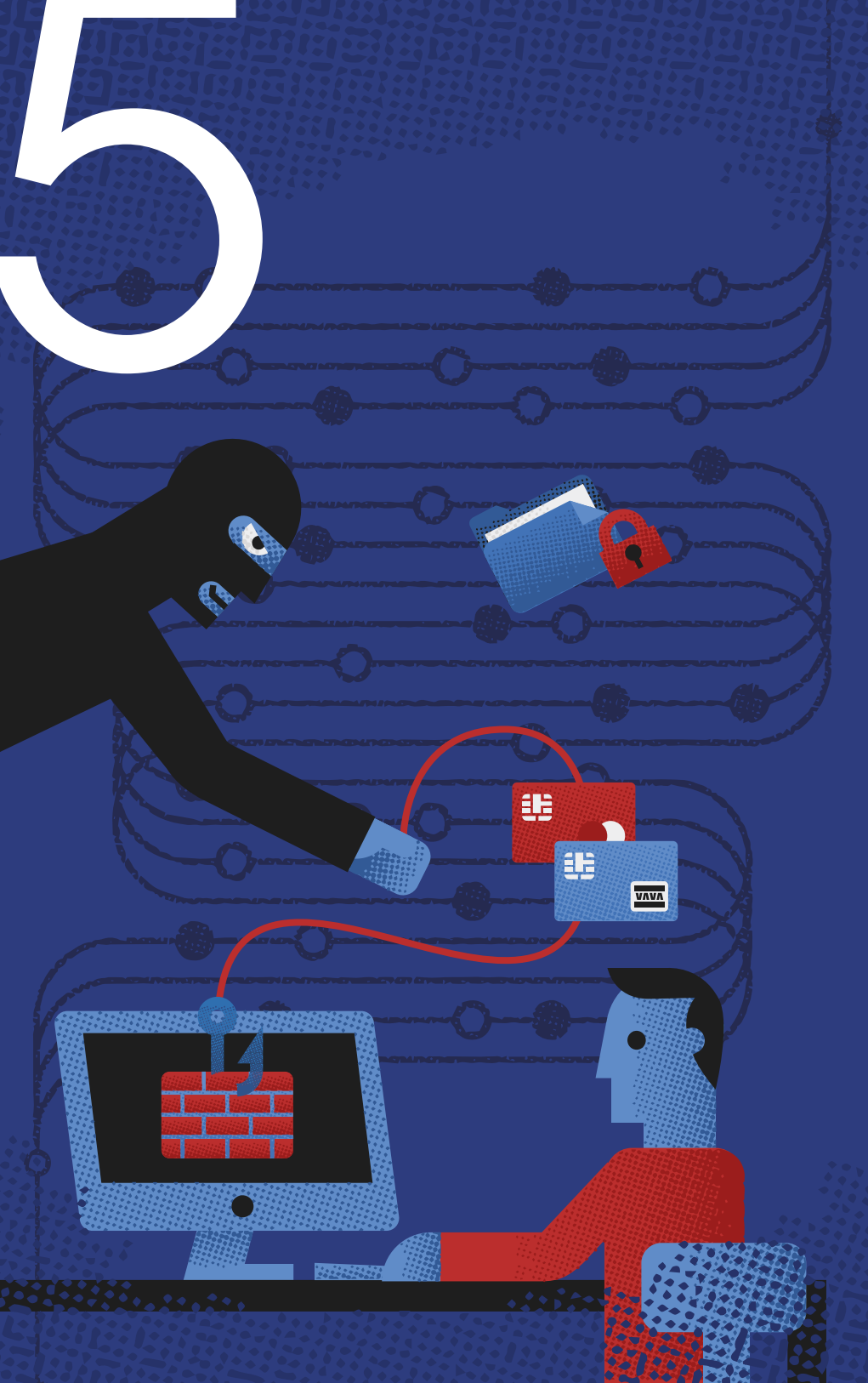
Explorative studies indicate that hackers start at a very young age, are influenced by their social network, and that there

are no differences in onset and persistence between traditional offenders and hackers (Bachmann, 2011; Chiesa et al., 2008; Hutchings & Clayton, 2016; Ruiter & Bernaards, 2013; Sarma & Lamb, 2013; Steinmetz, 2015a). Moral development ensures that most eventually stop (Gordon, 1994, 2000; Van Beveren, 2001; Voiskounsky & Smyslova, 2003). Bachmann (2010) indeed shows that hackers hack more when they have no job because it takes a long time to execute these hacks and they have less to lose if they do not have a job. Some hackers also claim they would stop if they get a good job in the IT sector, where they can use their skills legally (Chiesa et al., 2008). However, traditional protective factors such as work and school, especially in the IT sector, may offer the opportunity to commit cybercrimes (Leukfeldt et al., 2010; Randazzo et al., 2005; Turgeman-Goldschmidt, 2008, 2011b; Willison, 2006; Xu, Hu & Zhang, 2013). Finally, a study into the criminal careers of offenders involved in cyber-enabled crimes shows that fraudsters that use the internet to commit their crime are more likely to have a criminal record than fraudsters who only commit their crime offline (respectively 18% and 11%). Fewer offenders who were prosecuted for making online threats, however, had a criminal record compared to offenders who were prosecuted for making offline threats (respectively 19% and 31%) (Montoya et al., 2013). This implies that, when it comes to threats, the internet enables more "ordinary" people to make threats. With regard to fraud, it can be said that existing fraudsters are expanding their criminal activities to the online world (see Motoya et al., 2013).

Research into why people start, continue or stop committing cybercrimes is scarce. Are criminal careers of cybercriminals similar to those of offline offenders? And are cybercriminals specialists or all-rounders? Further, it is not known whether we are dealing with "new" offenders, or "old" offenders who have expanded their territory to the online world. This is due to the limitations of samples used in current studies and to the fact that there are only a few studies that make

a statistical comparison with traditional crimes. Longitudinal studies are completely lacking.

Furthermore, studies indicate that offenders not only commit cybercrimes, that traditional offenders sometimes switch to cybercrimes or that offline networks are used to recruit people who have the right skills to commit cybercrimes. Finally, traditional crimes increasingly have a digital component. This is in line with the Koop's observation (2017) that offline and online situations are merging more and more. This is referred to "the onlife world." It is important to gain more insight into exactly how cybercrimes and conventional crimes are intertwined. This intertwinement of the offline and online world with regard to careers of cybercrime offenders has not been studied yet.


5
VAVA

CYBERCRIMINAL NETWORKS

Rutger Leukfeldt, Christianne de Poot, Maite Verhoeven, Edward Kleemans, Anita Lavorgna

Characteristics of individuals

When we look at characteristics of individuals within cybercriminal networks, a combination can be seen of, on the one hand, a new type of offender and, on the other hand, offenders who have been active in the criminal world for a long time (Leukfeldt et al., 2016, 2017a, 2017b; Odinot et al., 2016). The new type of offenders includes criminals that were not previously found among traditional organized criminal groups, namely young offenders, offenders with an IT background, and ill or disabled offenders who barely leave their homes. Odinot et al. (2016) conclude that the characteristics of offenders that are important in the offline world, such as age, physical health, and social behavior, are less important within cybercriminal networks.

Research on "new players" in organized crime is needed. Traditional data sources have limitations that are further complicated by the anonymity the internet provides, which makes it difficult to identify (all) members of cybercriminal networks. When analyzing police files, for example, offenders who have not been detected by law enforcement agencies are not included in analyses. Alternative online data sources and advanced data collection methods are needed to gain insight into these offenders. One way of doing this is to analyze criminal activity on forums. Another way is collaborating with cybersecurity companies that monitor parts of the internet for their customers.

Origin and growth

Traditionally, social ties play an important role in the origins and growth processes of criminal networks (e.g., Bouchard & Morselli, 2014; Kleemans & De Poot, 2008). Social ties are strongly clustered and limited to, for example, a region or country. However, in the online world there are no geographical distances to be bridged in order to come into contact with other offenders; distance, location and time are no longer limiting factors. Compared to the offline world, it is relatively easy for offenders to be part of different criminal networks and to step in and out of collaborations with just a few clicks. Indeed, studies show that the process to get into a criminal group may be different in the digital world (e.g., Soudijn & Zegers, 2012; Yip et al., 2012). Newcomers on forums, for example, are able to come into contact with existing members quickly and are able to get a more central position relatively quickly. In contrast to physical networks, actors with a central position within networks seem to be less important. Apparently, in a virtual setting it is easier to connect to others than in a physical setting.

Several recent studies show that cybercriminal networks use offline social ties as well as online meeting places to come into contact with suitable co-offenders (Leukfeldt, 2014; Leukfeldt et al., 2016, 2017a; Odinot et al., 2016). The recruitment process can be divided into two main categories. The first main category is the traditional model: offline social contacts. Two subcategories can be distinguished: growth entirely through offline social contacts, and offline social contacts as a base and online meeting places to recruit specialists. The second main category is growth based on online meeting places. Again, two subcategories can be distinguished: growth entirely through online meeting places, and online meeting places as a base and offline social contacts for much needed local contacts (for example, money mules which are used to obscure the financial trail from victims to

core members of criminal networks). Networks that are able to make full use of the capabilities of these online meeting places seem to be able to expand their criminal capabilities quickly and are able to become international players in a relative small group (Leukfeldt et al., 2016, 2017a, 2017b).

Digitization provides new pathways into criminal networks. The effects of these new pathways on the structure and duration of criminal networks and criminal careers of individual members, for example, remain unclear. Examples of prolonged interaction on online forums can be seen. Core members of cybercriminal networks spend much of their time in chat rooms, meeting like-minded people and building relationships. With a whole new generation of digital natives coming up, it is likely that online social ties will become increasingly important in the development of cybercriminal networks. Research on differences and similarities between offline and online social ties, and their impact on the origins and growth processes and the functioning of cybercriminal networks, is needed.

Furthermore, countries that were part of the former Soviet Union are often seen as hotspots for cybercriminal networks (Bhattacharjee, 2011; Jones, 2010; Kshetri, 2013). Allegedly, many offenders or groups of offenders, including the highly skilled malware developers, operate from within these countries. Further research is needed into the involvement of Russian and East European cybercriminals and the factors that play a role in their alleged over-representation.

Structure

The internet offers an opportunity structure for decentralized flexible networks of offenders who distribute work based on knowledge and skills (see, for example, Odinot et al., 2016). Case studies suggest that within cybercriminal networks the importance of traditional central actors, who have the role

of bridge builder, diminishes (Decary-Hétu & Dupont, 2012; Decary-Hétu et al., 2012; Holt & Smirnova, 2014; Lu et al., 2010; Motoyama et al., 2013; Soudijn & Monsma, 2012; Yip et al., 2012). However, recent studies also show that cybercriminal networks still have dependency relationships (Leukfeldt et al., 2016, 2017a, 2017b). Most of the networks have a more or less stable group of core members who commit crimes together over an extended period of time. The core members of these networks often know each other from the offline world and recruit only a few specialists through online meeting places. A minority of networks could be labeled as ad hoc networks that were forged in online meeting places to execute one-off attacks.

An important question is how relevant the function of central nodes within cybercriminal networks will remain in the future. There is little research on the structure of cybercriminal networks, but studies do suggest that such nodes are diminishing in importance. What is more important for cybercriminals: the establishment of ad hoc alliances to quickly carry out attacks or finding a reliable group of accomplices to work with for a longer period of time? A better understanding of the organizational structure of cybercriminal networks will provide clues for opportunities to disrupt these networks. On which actors (and processes) do networks rely the most? Which actors are most difficult to find and replace?

Cybercriminal meeting places

Physical meeting places, such as a bar or clubhouse, play an important role within the origins and growth processes of criminal networks. These meeting places are of great importance when explaining crime, because their venues provide structure and continuity, and ensure that newcomers are able to connect with other members and become part of existing criminal networks (Felson, 2003, 2006). The internet has

its own criminal meeting places, for example, forums where hackers meet to exchange information or make plans to carry out attacks. To a certain extent, forums facilitate the origin and growth of cybercriminal networks. Indeed, in order to carry out successful attacks, offenders with all sorts of knowledge and skills are needed. Some criminals are, for example, good at developing malware, but do not have the skills to launder the money made from their criminal activities.

Members of cybercriminal networks spend much of their time in criminal and non-criminal chat rooms and forums, where they meet like-minded people and build relationships. Little is known about involvement mechanisms into cybercriminal networks and the role of forums in the origins and growth processes. For example, we do not know how curious loners who hang out on non-criminal forums end up in cybercriminal networks. Research into these involvement mechanisms is needed to better understand the origins and growth processes of cybercriminal networks.

Existing offline cultures, communities and social relationships appear to be important in online forums (Ablon et al., 2014). Aspiring members of invite-only forums, for example, have to have existing contacts with members of that forum: either online ties gained on other forums or chat channels, or offline ties that originated in the members' community or social cluster. Furthermore, not all members of the network are connected to one another (Holt & Smirnova, 2014). It is therefore questionable whether using forums removes the restrictions of the social network. New members have to already know someone in that particular criminal world. There is a lack of insight into the process of how aspiring cybercriminals enter open and closed forums.

Furthermore, it is necessary to conduct in-depth research on interactions on forums. These analyzes must go beyond the existing social network analyzes and descriptions of forums. For example, little is known about the type of offenders that

uses forums (from novice to expert), the number of attacks that originate from forums and how important forums are for the functioning of cybercriminal networks. Are forums, for example, only important for making initial contacts? Do subsequent interactions mainly take place outside the forum? And are forums populated by petty thieves who buy credit card credentials and curious young people who experiment with cybercriminal tools? Or are we dealing with professionals who systematically attack organizations in constantly changing compositions?

Cybercriminal markets

Most of the cybercriminal meeting places can be seen as criminal markets where all sorts of goods and services are traded. Different categories can be distinguished: (1) stolen data including credit card credentials, bank accounts details and PayPal accounts, and identity documents; (2) cybercriminal tools, such as, phishing kits, malware, botnets and DDoS attacks; (3) services such as escrow services that can be used to make secure transactions, exchangers that convert virtual money into real money, and bullet proof hosting; and (4) illegal trade in the more traditional illegal goods, such as, drugs, medication and weapons.

Although some researchers have attempted to estimate the size of specific online cybercrime markets (Dhanjani & Rios, 2008; Holtz et al., 2009), this seems to be an impossible task due to the variety of goods on offer, the uncertainty about differences between asking price and sale price (deals are usually closed outside the forum), and the supply of fake or outdated data and tools (Herley & Florencio, 2009; Holt & Smirnova, 2014). Despite all of this, it is important to understand the scale of online cybercrime markets, and to better understand the business models of cybercriminals active on these markets.

Trust

Finding reliable vendors is of great importance for the functioning of online criminal meeting places. There are several mechanisms to ensure that reliable members can be found. Firstly, having the appropriate reputation is required for entering closed forums. To access these forums, potential members are screened by administrators (or members appointed by the administrator) and they have to prove that they are active cybercriminals, for example, by providing stolen credit card data or a tutorial they have written (Ablon et al., 2014; Holt et al., 2015; Lusthaus, 2012; Soudijn & Zegers, 2012; Yip et al., 2013). Furthermore, members can earn all sorts of statuses that can be used to separate the reliable from the unreliable members. Sellers, for example, can get the status of "trusted seller" after getting good reviews from the official reviewers of the forum (Chu et al., 2010; Decary-Hétu & Dupont, 2013; Holt, 2013; Holt & Smirnova, 2014; Holt & Lampke, 2010; Lu et al., 2010; Motoyama et al., 2013; Peretti, 2008; Soudijn & Monsma, 2012; Yip et al., 2013). Finally, many forums have rating systems in which buyers rate and review the data, tools and services they purchased (Ablon et al., 2014; Chu et al., 2010; Dupont et al., 2016; Decary-Hétu & Dupont, 2012, 2013; Holt, 2013; Holt & Smirnova, 2014; Holt et al., 2015; Herley & Florencio, 2009; Lusthaus, 2012; Motoyama et al., 2011; Soudijn & Zegers, 2012; Wehinger, 2011; Yip et al., 2013). Other members now know that they are dealing with someone that sells the good stuff. The reviews and status are related to the online names used by members. These online handles, therefore, are of great importance to cybercriminals (Lusthaus, 2012).

The true importance of rating systems for the functioning of online meeting places is unclear. Rating systems rely heavily on the willingness of buyers to make reviews (Holt et al., 2015); if members do not give reviews, the good and bad sellers remain indistinguishable from one another. We know

that members of online meeting places do not always give reviews, therefore, the role of, for example, administrators who are able to award certain members a "high degree of reliability" status might be more decisive for determining reliability of members than review systems (Decary-Hétu & Dupont, 2013; Dupont et al., 2016).

As finding reliable members is of great importance for the functioning of online meeting places and, therefore, cybercriminal networks, research is needed into which actors or mechanisms have the most impact on trust in online meeting places. Experiments on online meeting places can be done to find out exactly how offenders establish trust, how these processes can be disrupted and what the displacement effects of interventions are.

Involvement of traditional organized crime groups

Little is known about the involvement of traditional organized crime groups in the execution of cybercrimes. While an increasing number of publications note that the internet is a tool exploited by organized crime groups (see, among others, Europol 2014, 2016), it seems they do not pay enough attention to the modalities and the extent to which traditional organized crime groups are exploiting some of the new opportunities provided by the internet to commit crimes, for instance, crimes in which the internet is used as a primary crime facilitator but is not necessarily an inherent part of the criminal activity. Indeed, apart from anecdotal evidence, there is still little research on which types of groups use the internet, to what degree, and for what types of activities (Lavorgna, 2015). Lavorgna and Sergi (2014) explored this question with regard to different Italian organized crime groups, and suggested that mafia-type groups operating in their traditional territories are not (yet) significantly exploiting the internet, probably because the social opportunity structure they rely on does not match very well with internet

usage and apparently it still works well enough that they do not feel the need to make any relevant changes. However, when mafia groups are operating in non-traditional territories, they are more open and quick to embrace new criminal opportunities, including online opportunities.

Empirical research on the involvement of traditional organized crime groups in the execution of cybercrimes is needed. Specifically, it is important to carry out comparative research considering differences (and explanations about these differences) on the diverse use of IT by different types of organized crime groups and in different territories.

Organized crime groups that are involved in trafficking activities have largely benefited from criminal opportunities the internet provides. In this case, the internet has affected criminal markets in a significant way, for instance, boosting certain trafficking flows more than others and opening the way for criminal niche markets. Moreover, where a structured criminal association was once needed because a minimum degree of sophistication was necessary in order to commit certain crimes, some organizational layers now do not seem to be fundamental anymore: very loose organizations are involved in serious trafficking activities (Lavorgna, 2015).

While recent research extensively focused on some of the internet-facilitated criminal markets (first and foremost, drug markets) other criminal activities have so far been overlooked. Furthermore, new research is needed to look specifically at the social dynamics regulating the choice of these organized crime groups to move (at least partially) online.

Offline side of cybercrime

Cybercrime is often seen as something global that only takes place in the virtual world. However, the offline world can certainly still be important. Research shows that members of

some cybercriminal networks are located in the same offline social cluster – even when executing cybercriminal attacks all over the world (Broadhurst et al., 2014; Leukfeldt et al., 2016, 2017a, 2017b; Odinot et al., 2016). Working with trusted acquaintances from the offline world could potentially have many advantages over working with potentially unreliable actors from all over the world who are only know by their online handle. Furthermore, not all cybercriminals only commit cybercrimes; studies show that cybercriminals are often also involved in all sorts of offline crimes (Hollinger, 1988; Leukfeldt et al., 2016, 2017b; Ruiter & Bernaards, 2013; Van der Broek et al., 2016).

Future research should also explicitly focus on the offline side of cybercrime. By only focusing on the new online aspect of the crime, a limited and distorted view of cybercriminals and cybercriminal networks is created.


6

VICTIMS

Jurjen Jansen, Marianne Junger, Joke Kort, Rutger Leukfeldt, Sander Veenstra, Johan van Wilsem, Sophie van der Zee

Nature, extent and impact on individuals

It is clear that cybercrime is a growing problem and that many people are being victimized. The latest figures from Statistics Netherlands, for example, show that in one year, 5.1 percent of the Dutch population fell victim to hacking, 3.5 percent fell victim to online consumer fraud, and 0.6 percent fell victim to identity fraud (CBS, 2016). In comparison, the highest percentages of victimization from traditional crimes in the Netherlands were bicycle theft (4%), burglary or attempted burglary (3%) and violence (2.2%) (CBS, 2016). Furthermore, prior victim studies show that individuals suffer from many more types of cybercrime: 16.7 percent of Dutch internet users fell victim to malware (with financial damages), 1.1 percent fell victim to cyberstalking and 0.7 percent fell victim to cyber threat (Domenie et al., 2013).

Although it is clear that victimization from some types of cybercrime is high, we fail to understand the nature, extent and impact of all types of cyber-dependent crimes and cyber-enabled crimes. Only a few specific types of cybercrime are measured annually. This makes it impossible to determine trends in cybercrime.

In order to gain insight into the entire spectrum of cybercrimes, it is necessary to develop instruments to periodically measure the nature, extent and impact of victimization of cybercrime. Victim surveys are generally used to gain insight into the nature and extent of victimization. However, these traditional victim surveys, which have been carried out over

decades, have little room to add extra questions related to cybercrime victimization. Because of this, for example, we know that hacking is one of the most common crimes in the Netherlands, but insight into the nature of these hacking incidents and the consequences for victims and society is lacking. Furthermore, the extent to which this method is suitable for measuring victimization of, for instance, malware is not known. Therefore, research into new methods and datasets is needed. Analyzing respondents' computers, for example, could provide a better picture of malware infections. It may also provide insight into the security measures installed by victims (see, for example, Anderson & Agarwal, 2010). Furthermore, computer log files can be used to study real rather than reported respondent behavior.

Nature, extent and impact on organizations

Knowledge about the nature, extent and impact of victimization among organizations is scarce. Virtually no research has been done into organization-specific cyber risks (Hernandez-Castro & Boiten, 2014; McGuire & Dowling, 2013; Schaper & Weber, 2012; Veenstra et al., 2015). Many estimates about victimization are made based on isolated data streams and case studies that are extrapolated to the whole of society. So far, estimates vary and are under as well as over reported (Anderson et al., 2013).

Recent Dutch research shows that small and medium-sized enterprises (SMEs), as well as freelancers, are active internet users who are highly dependent on IT systems. The majority of entrepreneurs take various technical measures against cybercrime (such as virus scanners or protecting Wi-Fi networks). Nevertheless, 28.5 percent of Dutch SMEs and 27.9 percent of one-man businesses fell victim to one or more forms of cybercrime (Veenstra et al., 2015). The extent of cybercrime victimization is comparable to that of traditional crimes among organizations (see, for example WODC, 2011). The

most common forms of cybercrime that entrepreneurs face are malware, internet fraud, phishing and hacking (Veenstra et al., 2015).

Research methods must be developed that can be used to systematically gain insight into the nature, extent and impact of victimization among organizations. This is needed to understand victimization and the economic and social consequences. Future studies should include characteristics, such as size of the organization and the sector of the organization, and factors, such as, cybersecurity measures and security training among employees.

Besides traditional victim surveys, online data or data from internal networks at organizations can be used to determine the nature and extent of cybercrime victimization and to map user behavior. Furthermore, data from hosting providers, for example, can be used to gain insight into the state of an organization's security and contamination of its content on servers (see, for example, the work of Van Eeten et al. (2010) on spam levels at ISPs). Finally, data from organizations, such as the Dutch National Cyber Security Center (NCSC), or hotlines, can be used to gain more insight into cyber-related incidents.

Reporting cybercrime

Even though the prevalence of cybercrime has increased rapidly and cybercrime has become part of everyday life of citizens during the last two decades, a major problem remains: victims of cybercrime are far less likely to report their victimization to the police than victims of traditional crime are. This is true for both individuals (13.4%, Domenie et al., 2013) and organizations (12.8%, Veenstra et al., 2015). However, it is of great importance that victims report these crimes to the police. Not only is this often necessary for starting a criminal investigation, it also increases the knowledge of the number

and types of crimes that are committed. Therefore, increasing victims' willingness to report crimes leads to more police investigations (and in turn to a better chance of catching the criminal) and a better understanding for developing countermeasures against the most common crimes, or crimes with the highest impact.

Currently, there is a lack of insight into the economic factors (costs and benefits) and the psychological factors (emotions and attitudes) that influence willingness to report crimes by individuals as well as organizations. Therefore, research into factors that influence the willingness to report crime is needed. It is important to differentiate between the various types of victims (e.g., individual citizens, small and medium-sized enterprises, international organizations) and different types of cybercrime.

Risk factors

The risk of falling victim to cybercrime is related to various personal and environmental characteristics. Dutch studies on victimization risk factors for various cybercrimes, such as hacking, phishing, online threats, online fraud and identity fraud, show that young people, people who spend a lot of time online, and impulsive people are more at risk of falling victim to most of these cybercrimes (Domenie et al., 2012; Jansen & Leukfeldt 2015; Jansen & Leukfeldt, 2016; Jansen et al., 2013; Leukfeldt 2014, 2015; Paulissen & Van Wilsem, 2015; Van Wilsem, 2011, 2013). Furthermore, researchers found that openness, extroversion, lack of self-control, thrill seeking, impulsivity and neuroticism are related to an increased chance of becoming a cybercrime victim (Halevi, Lewis & Memon, 2013; Modic & Leah, 2011; Ngo & Paternoster, 2011).

Routine activities of victims also seem to be related to cybercrime victimization. Examples of routine activities that lead to increased risk include being online more, opening

attachments from unknown sources, clicking on pop-ups, internet banking, online purchases, and not having up-to-date antivirus software (Anderson, 2006; Bossler & Holt, 2009; Choi, 2008; Hutchings & Hayes, 2009; Jansen & Leukfeldt, 2016; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Leukfeldt, 2014; Leukfeldt, 2015; Ngo & Paternoster, 2011; Pratt & Holtfreter Reisig, 2010; Van Wilsem, 2013).

Although quite a lot of research has been done on risk factors related to cybercrime victimization, current studies have some major limitations. Studies have different outcomes due to differences in their scope, for example, the types of cybercrimes included and the number of variables measured, and methodological limitations (use of small and/or non-representative samples). Although some psychological factors, such as self-control, have been studied a lot, other potential relevant factors, such as the Big Five personality traits (openness to experience, conscientiousness, extraversion, agreeableness and neuroticism) have not been explored in depth.

One of the most pressing issues is the fact that longitudinal studies are basically non-existent. As a consequence, the current studies based on cross-sectional data do not provide any insight into cause and effect relations (preventive measures can reduce risk, but victimization can also prompt victims to put preventive measures in place). Longitudinal data can also be used to study the impact of cybercrime victimization on online behavior, online risk perception and the risk of repeat victimization. This fits within a life course perspective on victimization, in which victimization is seen as an event that could lead to modification of behavior, which in turn has implications for future risks. Future studies should also look at whether specific groups, such as impulsive people, respond differently to victimization than the average victim – and how this can help explain patterns of repeat victimization.

Future research should take advantage of new methods and data sources. Actual behavior of end users can, for example, be studied using log files. This means that data must be collected from systems in homes, at the workplace, hosting providers, ISPs, or other relevant organizations.

Resilience

Humans are often described as the weakest link in cybersecurity. Therefore, it is important that people behave safely online (Shillair et al., 2015), for example, by being careful when sharing information online, by avoiding potentially dangerous websites, by using strong passwords and by keeping operating systems and other software up to date.

However, research into the correlation between attitudes and behavior in the field of privacy and online behavior has shown that although most people see cybersecurity as something important (Madden & Rainie, 2015) their actual behavior does not correspond to their attitudes (Spiekermann, et al., 2001; Broenink et al., 2009). Security measures are often viewed as a hygiene factor (Hassenzahl et al., 2010; IBM, 2014). i.e., as something that should be in order and that may potentially have negative results, but also something that should not bother you (Bada, Sasse & Nurse, 2015). In the context of an organization, the resilience of employees is also influenced by organizational factors such as corporate culture (Herath & Rao, 2009; Sohrabi Safa & Von Solms, 2016), management style (Soomro et al., 2016), human resource management (Wall, 2013) and budget (Bohme, 2010).

Researchers therefore have looked at how users can be motivated to take protective measures. It appears that confidence in their own ability to apply measures, the perceived effectiveness of a measure, and highlighting one's control or responsibility over online security is of great importance (Boehmer et al., 2015; Jansen & Van Schaik, 2016; Shillair et al., 2015).

Other studies focus on the more emotional side of prevention: making users aware, or perhaps afraid, of the possible consequences of disclosing information. However, this seems to have little positive effect on users (e.g., Kumaraguru, 2010; Purkait, 2012; Tembe et al., 2014; West, 2008). Also, psychological mechanisms, such as personal relevance, optimism bias and adverse effects, are important when it comes to target hardening. In general, it has been established that most people pay attention to warnings or other messages when these are perceived to be personally relevant, and that they do not pay attention to messages that lack personal relevance (Sagarin et al., 2002).

Research into the effectiveness of cybercrime and cybersecurity measures and training programs shows that making end users more resilient decreased the number of successful cyber-attacks (Bowen et al., 2012; Pattinson et al., 2012; Sheng et al., 2010). However, other studies have had different outcomes and the long-term effects of training programs are unknown (Caputo et al., 2014; Kumaraguru et al., 2009; Purkait, 2012). Bulee et al. (2016) find evidence that measures lose their effectiveness over time.

Insight into the long-term effects of technological measures is also lacking. Measures, such as blacklists or filters, have downsides, such as false positives (Hong, 2012; Leukfeldt et al., 2009; Ludl et al., 2007; Stol et al., 2008; Stol et al., 2009). Research into security indicators, such as the SSL lock or certificates, show that end users do not understand them or ignore them (Jakobsson, 2007; Dhamija et al., 2006). Furthermore, criminals can manipulate these indicators (Claessens et al., 2002).

Because of the lack of longitudinal studies, it is unclear what factors contribute to the long-term effectiveness of technical security measures, awareness campaigns, education and training programs. Future research into this will help increase the effectiveness of measures, training programs

and interventions on the various types of cyber-dependent and cyber-enabled crimes.

An important question is how security tools and processes can be designed in such a way that users are motivated and encouraged to act safely without interfering too much in their daily routines (also referred to as nudging and persuasive technologies). Key to answering these kinds of questions are the assets that need to be secure, the security tools and processes implemented to secure these assets, and the relation with psychological needs such as control, autonomy, efficiency and social constructs. IT systems at organizations seem particularly suitable for measuring actual behavior and the effect of implemented measures.

TACKLING CYBERCRIME

Floor Jansen, Bert-Jaap Koops, Jarmo van Lenthe, Eva Maas, Erik Planken, Bart Schermer, Wouter Stol, Maite Verhoeven

Introduction

Various organizations are involved in tackling crime. Boutellier (2005) uses a soccer metaphor to illustrate this. In the front line, citizens play a role. They have to behave safely and take precautions. In the midfield, organizations, such as housing associations and schools, play an important role. Although security is not the primary task of such organizations, they do have an important role in creating a secure environment. Organizations whose primary goal is to make society safer form the defense line. Examples include law enforcement agencies and private security companies.

The soccer metaphor can also be used with regard to the fight against cybercrime (see, for example, Boes & Leukfeldt, 2017; De Pauw & Leukfeldt, 2012). In the case of cybercrime, end users form the defense line. They themselves are able to secure their computer. In the midfield, ISPs, hosting companies and social media platforms play an important role. The defense consists of law enforcement agencies and, perhaps even more than with traditional forms of crime, private security companies and public-private partnerships.

End users

End users are important when it comes to keeping our digitized society safe and secure. First, their ability to neutralize

risks is important. For example, they have to be careful about sharing private information, they have to avoid dangerous online activities, use strong passwords and keep software up to date. Next, end users can take on various roles when it comes to protecting one another against cybercrimes (as the partner, educator, teacher, colleague, etc.). In addition, end users are an important source of information for law enforcement agencies. The information that law enforcement agencies have will only improve if victims or bystanders report cybercrimes. Finally, citizens are involved in various initiatives in which they are trying to create a safe digital society (e.g., activist groups and hotlines).

Chapter 4 lists what we already know about resilience and increasing the willingness to report cybercrime. Therefore, only some main aspects are discussed here. An important issue regarding end users and security measures is to find out how security measures and tools can be designed in such a way that users are motivated and encouraged to act safely without the measures interfering too much in their daily routines. It is known that the effects of security training programs decrease over time. Future research should, therefore, focus on identifying factors contributing to the long-term effectiveness of training programs.

With regard to the willingness to report cybercrimes, it is important to study the economic factors (costs and benefits) and psychological factors (emotions and attitudes) that influence willingness to report crimes by individuals as well as organizations. It is important to differentiate between different type of victims (e.g., individual citizens, small and medium-sized enterprises, international organizations) and different types of cybercrime.

With regard to online citizen initiatives, the following questions arise: What kind of initiatives exist at the moment and what are the legal and ethical limitations of such initiatives?

New super controllers

Traditionally, ISPs and hosting providers have played an important role as so-called super controllers. Super controllers are able to influence the behavior of others, for example, by using contractual governance, or by implementing security measures to protect their customers (for example, Wall, 2007). In recent years, new super controllers have arisen. Examples include Facebook, Google, Apple and Microsoft. Furthermore, the role of these organizations in the fight against cybercrime is also increasing. Besides the reactive assistance of law enforcement agencies in criminal investigations, these parties are increasingly being held accountable for their social responsibility in the prevention of illegal or unwanted statements (resulting in, for example, so-called voluntary notice and take-down policies).

Important research questions are: what role and what social or other responsibilities do super controllers have in the fight against the different types of cybercrime? Does the current legal framework for ISPs provide adequate safeguards for super controllers and enough space for detecting and combating cybercrime? And what impact does the public-private partnership between law enforcement agencies and super controllers have on the fundamental rights of citizens?

The criminal justice system

We live in a digitized society. The criminal justice system has to adapt to this. Studies into the functioning of the criminal justice system with regard to handling cybercrimes show that, apart from a few specialized teams, the police do not have the knowledge and skills to handle cybercrime cases effectively. But perhaps other factors also play a role, for example, capacity and organizational culture. Furthermore, it is questionable whether courts and lawyers are able to critically

assess the digital investigative methods used by the police (Leukfeldt et al., 2013; Stol et al., 2013).

The extent to which the criminal justice system is able to adapt to the ongoing digitization is not known. How effective is our criminal justice system in dealing with the various types of cybercrime? What are major bottlenecks and how can they be solved?

International criminal investigations

Because of the international character of many cybercrimes, criminal investigations into cybercrime require a rethinking of international legal frameworks. Traditional frameworks of collaboration between states are based on territorial sovereignty. Starting points are, therefore, often physical boundaries and a static location of evidence. However, the internet has fundamentally different characteristics. An important question is whether the current framework for international collaboration, as a link to national law enforcement, is still sufficiently equipped to guarantee the enforcement of the law (see, for example, Koops & Goodwin, 2014).

Nowadays, information can move rapidly, or may even be located at different places at the same time. Traditionally, criminal investigations are strictly linked to physical borders. As a result, at the moment, criminal investigations sometimes have to be stopped when it is not clear whether the IT infrastructure where the information is located, is in the Netherlands. In certain situations, new Dutch laws make it possible to continue parts of the criminal investigation, even if information is located outside the Netherlands. However, this problem applies to many European countries.

At the moment there is no clear picture of how other countries deal with the problems related to the international character of the various types of cybercrime. Are there explicit

investigative powers? Can the problem be solved through interpreting existing legal framework, or are other countries also developing new laws?

Another challenge relates to the patchwork of legal frameworks for collaboration with ISPs. The increasing digitization and development of cloud services, for example, makes access to the information that ISPs have vital for effective cybercrime investigations. ISPs are often located in either one or a small number of countries, whilst their users are located in many more countries. Also, ISPs and cloud computing services do not necessarily store user information in the country where the users are located. This creates situations where the cybercrime suspect is in one country, information on the suspect in the other, and the ISP who has to provide the information in yet another country. The current patchwork of rules on whether or not ISPs should provide information to law enforcement agencies does not constitute a transparent system. Collaboration is often on a voluntary basis, allowing ISPs to set their own rules about the conditions under which they cooperate with the criminal investigation.

Because of the high dependency of law enforcement agencies on ISP information, the development of a clear and effective legal framework is essential. What should a (European) framework for collaboration between ISPs and law enforcement agencies look like?

Preventive interventions

Only a few specific forms of cybercrime are individually recorded in the official record systems of the Dutch justice system. Cyber-enabled crimes in particular, tend to get lost in registration systems. Internet fraud, for example, is often recorded as fraud and not as cybercrime (Leukfeldt et al., 2010). As a consequence, a clear overview of the number of cybercrime-related convictions, penalties and recidivism is

missing. Further, there is still a lack of knowledge about the characteristics of cybercrime offenders and whether or not cybercriminals differ from perpetrators of traditional crimes (see Chapter 4).

Currently, we do not know how effective criminal investigation and prosecution is when it comes to the various types of cybercrime. Future research should not only map potential interventions and actors who should play a role in executing these interventions, but also evaluate the effectiveness of these interventions on the different types of cybercrime. Juvenile offenders deserve extra attention. What intervention methods are there that would make a first offender stop?

From a rational choice perspective, it is important to note that it pays to commit cybercrimes, perhaps even more than traditional crime (Boes & Leukfeldt, 2017; Holt, Smirnova, & Chua, 2016; Hutchings & Clayton, 2016; Lovet, 2006). Furthermore, the probability of detection and thus punishment is very low, probably lower than for traditional crime (Li, 2008; Rogers, 2001; Young et al., 2007). At the moment, it is not known how cybercriminals can be deterred, i.e., how we can make sure that the perceived costs are higher than the perceived benefits. Experimental research with honeypots shows that warning banners are not a guaranteed deterrent for hacking (Maimon et al., 2014). Criminal investigation and prosecution do seem to have an effect (Png & Wang, 2007), but it depends on the offender's motivation and level of risky behavior (Konradt et al., 2016), and only rational acting offenders who are aware of the possible consequences are affected by the probability of detection (Guitton, 2012).

Cybercrime is lucrative because the risk of being caught is low and the potential profit is high. Research on deterrence must be extended so that it becomes clear whether it makes sense to increase the probability of detection. This requires knowledge on the rational choices that cybercriminals make

and their motives for committing cybercrime. The different types of cybercrime and the motives related to them should be taken into account.

Alternatives for law enforcement

In addition to criminal investigations, other measures, such as victim notification, disruption, and damage mitigation, can be taken to make it harder for cybercriminals to carry out their attacks or to limit the impact of attacks. For example, software developers, owners of IT infrastructures or victims who do not yet know they are victims can be informed, so they can take measures to limit further damage. Furthermore, law enforcement agencies together with private parties that manage IT infrastructures are able to create barriers to stop offenders from using these IT services.

A recent example of this alternative approach is the NoMore-Ransom platform, a collaboration between the Dutch police, Europol and private security companies [nomoreransom.org], that aims to help citizens and organizations who are victim of so-called ransomware (using malware, cybercriminals encrypt files on the victims' computers. The victims have to pay to be able to use their data again.) The platform offers decryption tools and advice on how and where to report this crime. Also, potential victims are informed about what to do if they become a victim of ransomware.

Research into the possibilities of alternative interventions is limited. Important questions are: what intervention strategies are being used at the moment? Are they effective in preventing negative effects on victims and deterring potential offenders from committing cybercrimes? Which actors are involved in these alternative interventions and how do they work in practice? Is there a legal framework for existing public-private partnerships?

Interventions aimed at criminal markets

Hutchings and Holt (2016) provide an overview of interventions aimed at the disruption of online criminal markets. The authors make a distinction between interventions against the act, the actor and in the marketplace. When it comes to interventions against the act, measures are primarily aimed at disrupting opportunity structures. In order to do this, insight into so-called "crime scripts" – all the steps needed to commit a particular crime – is needed (see Hancock & Laycock, 2010; Hutchings & Holt, 2015; Leukfeldt et al., 2017b). Examples of such measures include monitoring banking transactions and anti-money laundering measures (e.g., discouraging providers of e-currencies to get involved in criminal activities) (Hutchings & Holt, 2016; Leukfeldt, 2016). Furthermore, criminal infrastructures, such as botnets, can be taken down. Botnets, networks of infected machines, are almost always a part of cybercriminal activities (Mielke & Chen, 2008; Schless & Vranken, 2013; Silva et al., 2012; Van der Wagen & Pieters, 2015). Measures against the actor focus on disrupting trust between offenders who are active on online meeting places (see also Chapter 5). This is called "lemonizing the market" (Herley & Florencio, 2009; Hoe et al., 2012). This can be done by so-called sybil and/or slander attacks with "fictitious" (unreliable) sellers or buyers who are used to create distrust in the market. The idea is that an uncertain market situation scares motivated offenders away. Finally, measures against the marketplace are all about taking down the online market places (see Hutchings & Holt, 2016).

Although a number of possible intervention strategies are described in the literature, research is needed into the legitimacy and effectiveness of these measures. Are there displacement effects? And which public and private actors should be involved?

Big data

The use of large data sets from multiple sources for criminal investigations is being subjected to increasing scrutiny (for example, Koops, 2009; De Vries & Smilda, 2014). The main problem in the Netherlands is that the criminal justice framework for the application of special investigative powers and the use of data within law enforcement agencies is governed by two different legal regimes that do not fit together (the Dutch Code of Civil Procedure (*Wetboek van Strafvordering*) and the Dutch Police Data Act (*Wet politiegegevens*). In short, when data enters the police organization legally in the context of a criminal investigation, this information can be used for anything. Hence, the increasing power of big data analysis may affect the privacy of suspects.

Relevant questions are whether more synergy is needed between the two legislative frameworks related to criminal investigations (the Dutch Code of Civil and the Dutch Police Data Act) and how this can be achieved. Furthermore, it is important to critically study the use of big data by law enforcement agencies. Indeed, big data also has disadvantages. Cause and effect relationships remain unclear and there will always be false positives and false negatives. Can big data be used effectively by law enforcement agencies in the fight against cybercrime?

Public private partnerships

Private organizations, including private security firms and detective agencies, are partners to the police when it comes to the fight against cybercrime. With the ongoing digitization of society, organizations that have large amounts of data about people, such as Google, Facebook, banks and eBay, also play an important role in criminal investigations.

Public-private partnerships in the fight against crime can be effective, but they also raise questions. Private parties proactively providing large data sets to the police (or other law enforcement parties) in order to detect cybercrime raises questions about privacy and data protection. Other relevant research questions on public-private partnerships are: what kind of information is exchanged between the police and their partners? How is this information being exchanged? How does this relate to the current legal framework (especially with regard to forensic principles)?

Future developments

Technological developments that are currently still in their infancy will have an impact on security and law enforcement in the near future. For example, the further digitization of motor vehicles and household products (internet of things). Society and law enforcement must prepare for this. Research questions in this context are: what digital developments will almost certainly affect security? What consequences does this have for law enforcement? How can parties involved in the fight against cybercrime prepare for this?

8

THE HUMAN FACTOR EXAMINED: DIRECTIONS FOR FUTURE RESEARCH

Rutger Leukfeldt

Introduction

Although research has been done into the human factor in cybercrime and cybersecurity, insight into the various aspects of these forms of crime is lacking. This is mainly due to the fact that the studies that have been done are often exploratory in nature, suffer from significant methodological limitations and focus on just a few of the many types of cybercrime.

This chapter describes the main findings of Chapter 4 to 7, where the state-of-the-art and key research questions are described related to offenders, victims and tackling crimes or incidents in which IT is the target or where IT plays a major role in the realization of the offense. Only the main lines for future research on the human factor in cybercrime and cybersecurity are presented in this chapter.

Overarching topics

LONGITUDINAL RESEARCH

One of the most pressing issues in research into the human factor in cybercrime and cybersecurity is the lack of longitudinal studies. The majority of studies that have been done are based on cross-sectional data (comparisons are done at a

single point in time). Longitudinal studies make comparisons over time and provide insight into cause-and-effect relationships. Longitudinal studies are needed into offenders (e.g., criminal careers, psychological characteristics), victims (e.g., online behavior, online risk perception and the risk of repeat victimization) and tackling cybercrime (e.g., the long-term effects of interventions, training programs and awareness campaigns).

THE OFFLINE SIDE OF CYBERCRIME

Cybercrime and cybersecurity is often seen as something global that takes place only in the virtual world. However, the offline world is still important when it comes to cybercrime. Research, for example, shows that offenders sometimes not only commit cybercrimes but are also involved in offline scams or drug smuggling; traditional offenders sometimes switch to cybercrimes; and offline networks are used to recruit people who have the right skills to commit cybercrimes. Indeed, the online world and offline world are intertwined. Future research should also explicitly focus on the offline side of cybercrime. Focusing on the new online aspect of the crime alone creates a limited and distorted view of cybercrime, cybersecurity incidents, cybercriminals and cybercriminal networks.

THE DARK FIGURE OF CYBERCRIME

For all types of crime, there is a dark figure. Existing data from organizations within the criminal justice system do not reflect the extent of crime. The dark figure includes offending, victimization and the extent of the damage. The dark figure for cybercrimes is considerably higher than that of traditional crimes. Because of this, basic information about, for example, the nature and extent of offending and victimization in the entire spectrum of cybercrimes is lacking, the long-term consequences for victims are not known, and is it impossible to determine trends. Research is needed to determine whether

traditional methods, such as victim and offender surveys, can be used to study the dark figure for cybercrimes. Also, the usability of new research methods and online and offline datasets have to be tested.

THE ENTIRE SPECTRUM OF CYBERCRIMES

There are various types of crimes or incidents in which IT is the target or where IT plays a major role in the realization of the offense. For future studies, the different types of crime and the characteristics related to them must be taken into account. The motivations and choices of offenders, and opportunities for interventions related to motivations may vary considerably for an individual hacker who hacks for recognition, a script kiddie who typically uses tools created by others without overseeing the consequences of their actions, and traditional organized crime groups that hire IT specialists to commit cyber-attacks. Future studies, therefore, should include the various types of crimes or incidents in which IT is the target or where IT plays a major role in the realization of the offense.

Offenders

THE CHARACTERISTICS OF CYBERCRIME OFFENDERS

It is not known whether cybercriminals are a new type of offender, or whether they are traditional offenders on new turf. There are several exploratory studies on the characteristics of cybercriminals, but these often have significant methodological limitations and/or focus on a limited number of cybercrimes. We therefore do not know exactly which characteristics are significant, and it is still unclear exactly how these characteristics are related and interact with, for example, IT knowledge or other specific characteristics of committing cybercrimes. Longitudinal studies that include the various forms of cybercrime are needed to map both demographic and psychological characteristics of cybercrime offenders.

THE SOCIAL AND CRIMINAL NETWORKS OF CYBERCRIME OFFENDERS

In addition to demographic and psychological characteristics of offenders, their social and criminal networks are related to criminal behavior. Explorative studies show that this applies to cybercrime as well. The knowledge required to commit cybercrimes can, for example, be learned from friends. Knowledge can also be gained from online networks, for example, on forums or chat channels. It seems that both online and offline social contacts are important, but exactly how these social contacts are related to committing cybercrime remains unclear. Longitudinal studies into offline, as well as online, social networks are needed to gain insight into the role of social networks in relation to cyber-dependent crimes and cyber-enabled crimes.

THE CRIMINAL CAREERS OF CYBERCRIME OFFENDERS

Understanding the characteristics of the criminal careers of cybercriminals and the processes that prompt them to start, continue or stop such behavior is relevant to developing effective prevention measures. Traditional life course research focuses on the question of when people start and stop criminal behavior, often by looking at factors associated with coming of age, such as a job, a house or a partner. The most reliable way to gain insight into this is through longitudinal studies. Currently, there are no longitudinal studies into the criminal careers of offenders involved in the various types of cybercrime.

CHARACTERISTICS OF CYBERCRIMINAL NETWORKS

Traditionally, social ties play an important role in the origins and growth processes of criminal networks. These social ties are strongly clustered and, therefore, limited to, for example, a region or country. However, in the online world, geographic distances do not need to be bridged in order to come into contact with other offenders. Digitization has ensured that

the pathways into criminal networks are somewhat different than before. However, its effects on the structure and duration of criminal networks are still unknown. Insight into this will provide pointers for possibilities for disrupting these criminal networks.

THE ROLE OF CRIMINAL ONLINE MEETING PLACES

In the formation of offline criminal networks, physical meeting places, such as a cafe, play an important role. The location provides structure and continuity: newcomers are able to establish links with existing members, enter existing criminal networks or create new criminal networks. The internet has its own criminal meeting places, such as forums where cybercriminals meet, buy technical tools or make plans to carry out attacks. In-depth research into interactions on forums is needed. These analyzes must go beyond the current social network analyzes and descriptions of forums. For example, there is a lack of insight into the number of attacks that originate from forums and how forums influence the functioning of cybercriminal networks.

FINDING RELIABLE CO-OFFENDERS

Finding reliable co-offenders to create criminal networks or to buy or sell cybercriminal tools and services are of great importance for the functioning of online meeting places. Online meeting places have several mechanisms that ensure that reliable members can be found, for example, there are different statuses and rating systems. However, the question is to what extent these rating systems are actually important for the members of a forum. Rating systems, for example, rely heavily on the willingness of buyers to give a review. However, buyers often do not cooperate well enough for review systems to work properly. Research is therefore needed into the actors and mechanisms that have the most impact on trust in online meeting places.

Victims

THE WILLINGNESS TO REPORT CYBERCRIMES

Victims of cybercrime (individuals as well as organizations) are far less likely to report their victimization to the police than victims of traditional crime. Currently, there is a lack of insight into the economic factors (costs and benefits) and psychological factors (emotions and attitudes) that influence willingness to report crimes on the part of individuals as well as organizations. Therefore, research into factors that influence willingness to report crime is needed. It is important to differentiate between the different types of victims (e.g., individual citizens, small and medium-sized enterprises, and international organizations) and different types of cybercrime.

FACTORS RELATED TO AN INCREASED CHANCE OF CYBERCRIME VICTIMIZATION

Young people, people who spent a lot of time online and impulsive people are more at risk of falling victim to cybercrime. It also appears that openness, extroversion, lack of self-control, sensation seeking, impulsiveness, and neuroticism are related to the risk of becoming a cybercrime victim. Finally, certain online activities, such as downloading and untargeted surfing, are related to victimization. Although quite a lot of research has been done on risk factors related to cybercrime victimization, there is no knowledge about the cause-effect relationships because of the use of cross-sectional data (preventive measures, for example, can reduce risk, but victimization also prompts victims to put preventive measures in place). Longitudinal studies that include background characteristics, psychological characteristics, as well as online behavior are needed to untangle these factors. Future studies should also include the entire range of cybercrimes to get a clear picture of factors related to the different types of cybercrime.

THE RESILIENCE OF END USERS

The resilience of end users, individuals as well as employees, seems to be an important protective factor in the prevention of cybercrime victimization. Researchers, therefore, have looked at how users can be motivated to take protective measures. For example, it turns out that the perceived effectiveness of a measure and highlighting one's responsibility for online security is important. Because there is no longitudinal research, insight into cause-effect relationships is lacking. In addition, studies indicate that the effectiveness of measures decreases over time. An important question is therefore how hardware and software can be designed in such a way that users are motivated and encouraged to act safely without interfering too much in their daily routines.

Tackling cybercrime

THE FUNCTIONING OF THE CRIMINAL JUSTICE SYSTEM IN A DIGITIZED SOCIETY

Studies into the functioning of the criminal justice system with regard to handling cybercrimes show that the police – apart from a few specialized teams – do not have the knowledge or skills required to effectively handle cybercrime cases. How effective is our criminal justice system in dealing with the various kinds of cybercrime? Furthermore, digitization is continuing at a rapid pace. Technological developments that are still in their infancy at the moment will have an impact on the criminal justice system and society in the near future. Society and the criminal justice system have to prepare accordingly. What digital developments will almost certainly affect security? And what are the consequences for the criminal justice system?

EFFECTIVE INTERVENTIONS

Cybercrime is lucrative because the risk of being caught is low and the potential profits are high. Research into deterring

cybercriminals has to be done in order to find out whether it makes sense to increase the probability of detection. This requires knowledge about the rational choices of cybercriminals, their motives for committing cybercrimes and their business models. There is currently no knowledge about the effectiveness of specific intervention measures aimed at preventing first-time offending or recidivism involving the various types of cybercrime and related motives.

EFFECTIVE ALTERNATIVE INTERVENTIONS

In addition to criminal investigations into cybercriminals, various actors can be used to make it harder for cybercriminals to carry out their attacks. For example, software developers, owners of IT infrastructures or victims who are not yet aware that they are victims can be informed so they can take measures to limit further damage. Also, IT structures used by cybercriminals can be disrupted. Despite the importance of alternative interventions, research on this topic is limited. Currently, there is no insight into effective interventions aimed at cyber-dependent crimes and cyber-enabled crimes.

THE ROLE OF PRIVATE PARTIES

Public-private partnerships in the fight against crime can be effective, but they also raise questions. Private parties proactive sharing large data sets with law enforcement agencies in the context of detecting cybercrime raises questions about privacy and personal data protection. What kind of information is currently being exchanged between private parties and the police? How is this information being exchanged? How does this relate to the current legal framework (especially with regard to forensic principles)? Another challenge relates to the patchwork of legal regimes for collaboration with ISPs. Due to the high dependency that law enforcement agencies have on the information that ISPs have, the development of a clear and effective legal framework is essential.

What should a legal framework for collaboration between ISPs and law enforcement agencies look like?

THE ROLE OF SUPER CONTROLLERS

Traditionally, ISPs and hosting providers have played an important role as super controllers. Super controllers are able to influence the behavior of others in order to reduce the risk of incidents, for example, by contractual governance or by installing security measures. Over the years, new super controllers have arisen. Examples include Facebook, Google, Apple and Microsoft. What role do these super controllers have in the fight against cybercrime? Does the current legal framework for ISPs provide sufficient safeguards for super controllers and is there enough space for cooperation with law enforcement agencies in the fight against cybercrime? And what effect on the fundamental rights of citizens do public-private partnerships between super controllers and law enforcement agencies have?

REFERENCES

Ablon, L., Libicki, M.C. & Golay, A.A. (2014). *Markets for Cybercrime Tools and Stolen Data. Hackers' Bazaar*. Santa Monica, CA: RAND Corporation.

Anderson, K.B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160-171.

Anderson, C.L. & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly 34*(3) A1-A15.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M.J.G., Levi, M., Moore, T. & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy*. Springer-Verlag Berlin Heidelberg.

Aransiola, J.O. & Asindemade, S.O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 759-763.

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1), 643-656.

Bachmann, M. (2011). Deciphering the hacker underground: first quantitative insights. In T.J. Holt & B.H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 105-126). New York: Information Science Reference.

Bachmann, M. & Corzine, J. (2010). Insights into the hacking underground. In T. Finnie, T. Petee & J. Jarvis (Eds.), *The Future Challenges of Cybercrime. Volume 5: Proceedings of the Futures Working Group 2010*. (pp. 31-41). Quantico, VA: FBI.

Bada, M., Sasse, M.A. & Nurse, J.R.C. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Retrieved from Oxford, UK: http://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf.

Bhattacharjee, Y. (2011). Why does a remote Town in Romania have so many Cybercriminals? *Wired*, *19*(2).

Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M. & Iamnitchi, A. (2014). Cheating in online games: A social network perspective. *Acm Transactions on internet Technology*, *13*(3) 9-25.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S. & Cotton, S. (2015). Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students, *Behaviour & Information Technology*, *34*(10) 1022-1035.

Boes, S. & Leukfeldt, E.R. (2017). Fighting Cybercrime: A Joint Effort. In M.R. Clark & S. Hakim (Eds.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 185-203). Cham: Springer International Publishing.

Bohme, R. (2010). Security Metrics and Security Investment Models. In I. Echizen, N. Kunihiro, R. Sasaki (Eds.), *Security Metrics and Security Investment Models*. Lecture Notes in Computer Science, vol. 6434, 10-24. Springer, Berlin/Heidelberg.

Bossler, A.M. & Holt, T.J. (2009). Online activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bossler, A.M. & Burrus, G.W. (2011). The general theory of crime and computer hacking: Low self-control hackers? In T.J. Holt & B.H. Schell (Eds.), *Corporate hacking and technology driven crime: social dynamics and implications*. PA: IGI Global.

Bouchard, M. & Morselli, C. (2014). Opportunistic structures of organized crime. In L. Paoli (Ed.), *The Oxford Handbook of Organized Crime*. Oxford/New York: Oxford University Press.

Boutellier, H. (2005). *Meer dan veilig. Over bestuur, bescherming en burgerschap*. The Hague: Boom Juridische uitgevers.

Bowen, B.M., Devarajan, R. & Stolfo, S. (2012). Measuring the Human Factor of Cyber Security. *Homeland Security Affairs*, *Supplement 5*, Article 2.

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cybercrime: An analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cybercriminology*, *8*(1), 1-20.

Broenink, E.G., Schultz, S., de Vries, A., Wolthuis, R. & Fransen, F. (2009). Veilig met gemak. (Internal TNO repport). TNO.

Bullee, J.W., Montoya, L., Junger, M. & Hartel, P. (2016). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention*. Paper presented at the Cyber Security R&D Conference (SG-CRC) 2016, Singapore.

Caputo, D.D., Pfleeger, S.L., Freeman, J.D. & Johnson, M.E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, *12*(1), 28-38.

CBS (2016). *IT, kennis en economie*. The Hague: Statistics Netherlands.

Chiesa, R., Ducci, S. & Ciappi, S. (2008). *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. Boca Raton: CRC Press.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Chu, B., Holt, T.J. & Ahn, G.J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line*. Technical Report for National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018. Available at http://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf.

Claessens, J., Dem, V., De Cock, D., Preneel, B. & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, (21), 253-265.

Décary-Hétu, D. & Dupont, B. (2012). The social network of hackers. *Global Crime 13*(3), 160-175.

Décary-Hétu, D. & Dupont, B. (2013). Reputation in a dark network of online criminals, *Global Crime*, *14*(2-3) 175-196.

Décary-Hétu, D., Morselli, C. & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among Warez hackers. *Journal of Research in Crime and Delinquency*, *49*(3), 359-382.

De Vries, A. & Smilda, F. (2014). *Social media: het nieuwe DNA. Een revolutie in opsporing*. Amsterdam: Reed Business.

Dhamija., R., Tygar, J.D. & Hearst, M. (2006). Why Phishing Works. *CHI '06 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581-590.

Dhanjani, N. & Rios, B. (2008). Bad sushi: Beating phishers at their own game. Paper presented at the *Annual Blackhat Meetings*, Las Vegas, Nevada.

Dietrich, D., Kasper, K. & Bulanova-Hristova, G. (2016). Literature review. In G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, Y. Werner and L. Korsell (Eds.), *Cyber-OC: Scope and Manifestations in selected EU member states*. Wiesbaden: BKA, Bra, WODC.

Dizon, M.A.C. (2016). *Breaking and remaking law and technology: A socio-techno-legal study of hacking* (Doctoral thesis). Tilburg: Tilburg University.

Domenie, M.M.L., Leukfeldt, E.R., Van Wilsem, J.A., Jansen, J. & Stol, W.P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. The Hague: Boom Lemma Uitgevers.

Donner, C.M., Marcum, C.D., Jennings, W.G., Higgins, G.E. & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165-172.

Dupont, B., Côté, A.M., Savine, C. & Décary Hétu, D. (2016). The ecology of trust among hackers. *Global Crime 17*(2), 129-151.

Europol (2014). *Internet facilitated organized crime (IOCTA)*. The Hague: European Police Office.

Europol (2016). *Internet facilitated organized crime (IOCTA)*. The Hague: European Police Office.

Felson, M. (2003). The process of co-offending. In M.J. Smith & D.B. Cornish (Eds.), *Theory for practice in situational crime prevention (volume 16)*. Devon: Willan Publishing, 149-168.

Felson, M. (2006). *The ecosystem for organized crime* (HEUNI paper no. 26). Helsinki: HEUNI.

Flores, W.R., Holm, H., Nohlberg, M. & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, *23*(2), 178-199.

Fotinger, C. & Ziegler, W. (2004). *Understanding a hacker's mind: a psychological insight into the hijacking of identities*. Krems: Donau-Universität Krems.

Goode, S. & Cruise, S. (2006). What motivates software crackers? *Journal of Business Ethics*, *65*(2), 173-201.

Gordon, S. (1994). *The generic virus writer*. Paper presented at the International Virus Bulletin Conference, Jersey.

Gordon, S. (2000). *Virus writers: the end of the innocence?* Paper presented at the International Virus Bulletin Conference, Orlando.

Gordon, S. & Ma, Q. (2003). *Convergence of virus writers and hackers: Fact or fantasy?* White paper. www.symantec.com.

Guitton, C. (2012). Criminals and cyber attacks: the missing link between attribution and deterrence. *International Journal of Cyber Criminology*, *6*(2), 1030-1043.

Halevi, T., Lewis, J. & Memon, N. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. *WWW 2013 Companion, May 13-17, 2013, Rio de Janeiro, Brazil*.

Hancock, G. & Laycock, G. (2010). Organised Crime and Crime Scripts: Prospects for Disruption. In K. Bullock, R.V. Clarke & N. Tilley. *Situational Prevention of Organised Crime*, pp. 172-192. Devon: Willan Publishing.

Hargreaves, C. & Prince, D. (2013). *Understanding cyber criminals and measuring their future activity: Developing cybercrime research*. Lancaster: Lancaster University.

Harvey, I., Bolgan, S., Mosca, D., McLean, C. & Rusconi, E. (2016). Systemizers Are Better Code-Breakers: Self-Reported Systemizing Predicts Code-Breaking Performance in Expert Hackers and Naïve Participants. *Frontiers in Human Neuroscience*, *10*(229). doi:10.3389/fnhum.2016.00229.

Hassenzahl, M., Diefenbach, S. & Goritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. Interacting with computers, *22*(5), 353-362.

Herath, T. & Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 106-125.

Herley, C. & Florencio, F. (2009) *Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy*. Microsoft TechReport nr MSR-TR-2009-34.

Hernandez-Castro, J. & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, *2014* (2), 5-8.

Hoe, S.C., Kantarcioglu, M. & Bensoussan, A. (2012) A Game Theoretical Analysis of Lemonizing Cybercriminal Black Markets. In J. Grossklags & J. Walrand (Eds.) Decision and Game Theory for Security, Berlin: Springer, 2012.

Hollinger, R.C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research*, *72*(3), 199-200.

Hollinger, R.C. (1993). Crime by computer: Correlates of software piracy and unauthorized account access. *Security Journal*, *4*(1), 2-12.

Holt, T.J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior 28*(2), 171-198.

Holt, T.J. (2013). Examining the Forces Shaping Cybercrime Markets Online. *Social Science Computer Review 31*(2), 165-177.

Holt, T.J. (2013). Exploring the social organization and structure of stolen data markets. *Global Crime*, *14*(2-3), 155-174.

Holt, T.J. & Kilger, M. (2008). Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers. wistdcs, pp.67-78, *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing*.

Holt, T.J. & Lampke, E. (2010). Exploring Stolen Data Markets Online: Products and Market Forces, *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T.J. & Smirnova, O. (2014). *Examining the Structure, Organization, and Processes of the International Market for Stolen Data*. Washington: US Department of Justice

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T.J. & Bossler, A.M. (2016). Technology and Violence. C.A. Cuevas & C.M. Rennison (Eds.), The Wiley Handbook on the Psychology of Violence. West Sussex: Wiley-Blackwell.

Holt, T.J., Burruss, G.W. & Bossler, A.M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Holt, T.J., Bossler, A.M. & May, D.C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, *37*(3), 378-395.

Holt, T.J., Smirnova, O. & Chua, Y.T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353-367. doi:10.1080/01639625.2015.1026766

Holt, T.J., Strumsky, D., Smirnova, O. & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*, 891-903.

Holt, T.J., Strumsky, D., Smirnova, O. & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology* (IJCC) *6*(1): 891-903.

Holt, T.J., Smirnova, O., Chua, Y.T. & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime 16*(2), 81-103.

Hong J. (2012). The state of phishing attacks, *Communications of the ACM*, *55*(1), 74-81.

Hu, Q., Xu, Z. & Yayla, A.A. (2013). Why college students commit computer hacks: Insights from a cross culture analysis. Paper presented at the *Pacific Asia Conference on Information Systems* (PACIS), Jeju Island, Korea.

Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20.

Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'net'? *Current Issues in Criminal Justice*, *20*(3), 1-20.

Hutchings, A. & Holt, T.J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology 55*(3): 596-614.

Hutchings, A. & Holt, T.J. (2016). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1) 11-30.

Hutchings, A. & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior, 37*(10), 1163-1178.

IBM (2014). *IBM Security Services 2014 Cyber Security Intelligence Index*.

Jakobsson, M. (2007). The human factor in phishing, *Privacy & Security of Consumer Information*, (7), 1-19.

Jansen, J. & Leukfeldt, E.R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, 24-31.

Jansen, J. & Leukfeldt, E.R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

Jansen, J. & van Schaik, P. (2016). Understanding precautionary online behavioural intentions: A comparison of three models. *Proceedings of the*

Tenth International Symposium on Human Aspects of Information Security & Assurance (HAIZA), 1-11.

Jansen, J., Junger, M., Montoya, A. & Hartel, P. (2013). Offenders in a digitized society. In W.P. Stol & J. Jansen (Eds.), *Cybercrime and the Police*. The Hague: Boom Lemma.

Jansen, J., Veenstra, S., Zuurveen, R. & Stol, W.P. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368-379.

Jones, J. (2010). *Profile of A Global Cybercrime Business – Innovative Marketing*. Microsoft Security Blog Retrieved from https://blogs.microsoft.com/microsoftsecure/2010/03/25/profile-of-a-global-cybercrime-business-innovative-marketing/. Last visited 23 February 2017.

Kerstens, J. & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior*, *37*(5), 585-600. doi:10.1080/01639625.2015.1060796.

Kleemans, E.R. & De Poot, C.J. (2008) Criminal Careers in Organized Crime and Social Opportunity Structure, *European Journal of Criminology*, *5*(1), 69-98.

Konradt, C., Schilling, A. & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, *58*, 39-46.

Koops, B.J. (2009). Technology and the Crime Society: Rethinking Legal Protection. *Law, Innovation and Technology 1*(1), 93-124.

Koops, B.J. (2017). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In B. Akhgar, & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*. DOI 10.1007/978-3-319-38930-1

Koops, B.J. & Goodwin, M.E.A. (2014). *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*. The Hague/Tilburg: WODC/TILT.

Kshetri, N. (2013). Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. *Crime, Law and Social Change*, *60*(1), 39-65.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. & Pham, T. (2009). School of Phish: A Real-Word Evaluation of Anti-Phishing Training. *SOUPS '09 Proceedings of the 5th Symposium on Usable Privacy and Security*. Article No. 3.

Lavorgna, A. (2015). Organised crime goes online: Realities and challenges, *Journal of Money Laundering Control 18*(2), 153-168.

Lavorgna, A. & Sergi, A. (2014). Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of internet technologies. *International Journal of Law, Crime and Justice 42*(1), 16-32.

Leukfeldt, E.R. (2014a). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking*, *17*(8), 551-555.

Leukfeldt, E.R. (2014b). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime 17*(4), 231-249.

Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. (Doctorate thesis) The Hague: Eleven International Publishers.

Leukfeldt, E.R. & De Pauw, E. (2012). Fighting cybercrime: an integral approach. In E.R. Leukfeldt & W.P. Stol (Eds.) *Cyber Safety: An Introduction*. The Hague: Eleven International Publishers.

Leukfeldt, E.R. & Stol, W.P. (2012). De rol van internet bij fraudedelicten. *Justitiële Verkenningen*, *38*(1) 108-120.

Leukfeldt, E.R. & Yar, M. (2016). Applying routine activity theory to cybercrime. A theoretical and empirical analysis. *Deviant Behavior*. DOI:10.1080/01639625.2015.1012409.

Leukfeldt, E.R., Domenie, M.M.L. & Stol, W.P. (2010). *Verkenning cybercrime in Nederland 2009*. The Hague: Boom Lemma Uitgevers.

Leukfeldt, E.R., Veenstra, S. & Stol, W.P. (2013). High volume cyber crime and the organization of the police: the results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, *7*(1), 1-17.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2016). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*. DOI:10.1093/bjc/azw009.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*. doi:10.1093/bjc/azw009

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017a). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9647-1.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017b). A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9646-2.

Leukfeldt, E.R., Veenstra, S., Domenie, M.M.L. & Stol, W.P. (2013). *De strafrechtketen in een gedigitaliseerde samenleving: een onderzoek naar de strafrechtelijke afhandeling van cyber crime*. De Bilt/Leeuwarden: PAC/NHL.

Leukfeldt, E.R., Stol, W.P., Kaspersen, H.W.K., Kerstens J. & Lodder A.R. (2009). Filteren op internet. De rol van de Nederlandse overheid in het blokkeren van kinderpornografische websites *Tijdschrift voor Veiligheid 8*(4) 36 - 50.

Li, X. (2008). The criminal phenomenon on the internet: Hallmarks of criminals and victims revisited through typical cases prosecuted. *University of Ottawa Law & Technology Journal*, *5*(1 & 2), 125-140.

Lovet, G. (2006). *Dirty money on the wires: the business models of cyber criminals*. Paper presented at the 16th Virus Bulletin International Conference, Montréal, Canada.

Lu, Y., Luo, X., Polgar, M. & Cao, Y. (2010). Social Network Analysis of a Criminal Hacker Community. *Journal of Computer Information Systems 51*(2) 31-41.

Ludl, C., McAllister, S., Kirda, E. & Kruegel, C. (2007). On the effectiveness of techniques to detect phishing sites. In M. Hämmerli B., R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2007. Lecture Notes in Computer Science, Volume 4579. Berlin, Heidelberg: Springer.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime 13*(2), 71-94.

Madden, M. & Rainie, L. (2015) Americans' Attitudes About privacy, Security and Surveillance, Retrieved February 23, 2017, from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Maimon, D., Kamerdze, A., Cukier, M. & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: an application of the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343.

Maimon, D., Alper, M., Sobesto, B. & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Marcum, C.D., Higgins, G.E., Ricketts, M.L. & Wolfe, S.E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

McGuire, M. & Dowling, S. (2013). Chapter 1: Cyber-dependent crimes *Cyber crime: A review of the evidence* (Home Office Research Report 75 ed., pp. 4-34).

Mielke, C.J. & Chen, H. (2008). Botnet and the Cybercriminal Underground. Paper presented at IEEE International Conference on Intelligence and Security Informatics. DOI: 10.1109/ISI.2008.4565058.

Modic, D. & Lea, S.E.G. (2011). How neurotic are scam victims, really? The big five and internet scams. *Paper presented at the 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology, Exeter, United Kingdom*.

Montoya, L., Junger, M. & Hartel, P. (2013). How 'Digital' is Traditional Crime? *European Intelligence and Security Informatics Conference*, *EISIC*, 12-14 August 2013, Uppsala, Sweden.

Moon, B., McCluskey, J.D. & McCluskey, C.P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, *38*(4), 767-772.

Moon, B., McCluskey, J.D., McCluskey, C.P. & Lee, S. (2013). Gender, General Theory of Crime and computer crime: An empirical test. *International Journal of Offender Therapy and Comparative Criminology*, *57*(4), 460-478.

Morris, R.G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T.J. Holt & B.H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 1-17). New York: Information Science Reference.

Morris, R.G. & Blackburn, A.G. (2009). Cracking the code: an empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, *32*(1), 1-34.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. & Voelker, G.M. (2013). An Analysis of Underground Forums. *IMC'11* 71-79.

Ngo, F.T. & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Odinot, G., Verhoeven, M.A., Pool, R.L.D. & De Poot, C.J. (2016). *Cybercrime, Organised Crime and Organised Cybercrime in the Netherlands:*

Empirical Findings and Implications for Law Enforcement. The Hague: WODC.

Palesh, O., Saltzman, K. & Koopman, C. (2004). Internet use and attitudes towards illicit internet use behavior in a sample of Russian college students. *CyberPsychology & behavior*, *7*(5), 553-558.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18-28.

Paulissen, L. & Van Wilsem, J. (2015) *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*. Amsterdam: Reed Business.

Peretti, K.K. (2008). Data breaches: What the Underground World of "Carding" Reveals, *Santa Clara Computer and High-technology Law Journal*, *25*(2), 345-414.

Png, I.P. & Wang, C.Y. (2007). The Deterrent Effect of Enforcement Against Computer Hackers: Cross-Country Evidence. Paper presented at the *Workshop on the Economics of Information Security*, Pittsburgh.

Pratt, T.C., Holtfreter, K. & Reisig, M.D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, 20*(5)*, 382-420.

Randazzo, M.R., Keeney, M., Kowalski, E., Cappelli, D. & Moore, A. (2005). *Insider threat study: illicit cyber activity in the banking and finance sector.* Pittsburg: Carnegie Mellon Software Engineering Institute.

Rogers, M. (1999). Modern-day Robin Hood or moral disengagement: Understanding the justification for criminal computer activity. Retrieved February 23, 2017, from http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=27457EF56CCB68392761A81B47A85D4D?doi=10.1.1.31.8031&rep=rep1&type=pdf.

Rogers, M. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. (doctoral thesis) Winnipeg: University of Manitoba.

Rogers, M., Seigfried, K. & Tidke, K. (2006). Self-reported computer criminal behavior: a psychological analysis. *Digital Investigation*, *6*(3), 116-120.

Rogers, M., Smoak, N.D. & Liu, J. (2006). Self-reported deviant computer behavior: A Big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior*, *27*(3), 245-268.

Ruiter, S. & Bernaards, F. (2013). Are crackers different from other criminals? A comparison based on Dutch suspect registrations. *Tijdschrift voor Criminologie*, *55*(4), 342-359.

Sagarin, B.J., Cialdini, R.B., Rice, W.E. & Serna, S.B. (2002). Dispelling the illusion of invulnerability: the motivations and mechanisms of resistance to persuasion. *Journal of personality and social psychology*, *83*(3), 526.

Sarma, M. & Lam, A. (2013). Knowledge creation and innovation in the virtual community – Exploring structure, values and identity in hacker groups. Paper presented at the 35th *DRUID Celebration Conference*, Barcelona, Spain.

Schaper, M.T. & Weber, P. (2012). Understanding Small Business Scams. *Journal of Enterprising Culture*, *20*(03), 333-356.

Schell, B. H. & Melnychuk, J. (2011). Female and male hacker conferences attendees: their autism-spectrum quotient (AQ) scores and self-reported adulthood experiences. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 144-168). New York: Information Science Reference.

Schless, T. & Vranken, H. (2013). Counter Botnet Activities in the Netherlands. A Study on organisation and effectiveness. *8th International Conference for internet Technology and Secured Transactions* (ICITST). DOI: 10.1109/ICITST.2013.6750238 ·

Seigfried, K. & Treadway, K.N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, *35*(10), 782-803.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Paper presented at *CHI 2010: Privacy Behaviors*, April 10-15, 2010, Atlanta, GA, USA.

Shillair, R., Cotten, S.R., Tsai, H.Y.S., Alhabash, S., LaRose, R. & Rifon, N.J. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, *48*, 199-207.

Silva, S.S.C., Silva, R.M.P., Pinti, R.C.G. & Salles, R.M. (2012). Botnets: A Survey, *Computer Networks*, *57*(2), 378-403.

Skibell, R. (2002). The myth of the computer hacker. *Information, Communication & Society*, *5*(3), 336-356.

Skinner, W.F. & Fream, A.M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, *34*(4), 495-518.

Sohrabi Safa, N. & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Sood, A.K. & Enbody, R.J. (2013). Crimeware-as-a-service-A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Soudijn, M.R.J. & Monsma, E. (2012). Virtuele ontmoetingsuimtes voor cybercriminelen. *Tijdschrift voor Criminologie*, *54*(4), 349-360.

Soudijn, M.R.J. & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime 15*(2-3), 111-129.

Spiekermann, S., Grossklags, J. & Berendt, B. (2001). E-privacy In 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior. *Proceedings of the ACM Conference on Electronic Commerce*, Tampa, Florida, USA, October 14-17, 2001.

Steinmetz, K.F. (2015a). Becoming a Hacker: Demographic Characteristics and Developmental Factors. *Journal of Qualitative Criminal Justice and Criminology*, *3*(1), 31-60.

Steinmetz, K.F. (2015b). Craft(y)ness: An Ethnographic Study of Hacking. *British Journal of Criminology*, *55*(1), 125-145.

Stol, W.P., Leukfeldt, E.R. & Klap, H. (2013). Policing a digital society. The state of affairs in the Netherlands in 2013. In W.P. Stol & J. Jansen (Eds.), *Cybercrime and the Police*. The Hague: Eleven International Publishing.

Stol, W.P., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2008) *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland*. The Hague: Boom Juridische uitgevers.

Stol, W.P., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2009) Governmental filtering of websites: the Dutch case. *Computer Law & Security Review* 25(3) 251-262.

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & behavior*, *7*(3), 321-326.

Tembe, R., Zielinska, O., Liu, Y., Hong, K. W., Murphy-Hill, E., Mayhorn, C. & Ge, X. (2014). *Phishing in international waters: exploring cross-national differences in phishing conceptualizations between Chinese, Indian and American samples*. Paper presented at the Proceedings of the 2014 Symposium and Bootcamp on the Science of Security, Raleigh, North Carolina, USA.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, *2*(2), 382-396.

Turgeman-Goldschmidt, O. (2011a). Between hackers and white-collar offenders. In T.J. Holt & B.H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 18-37). New York: Information Science Reference.

Turgeman-Goldschmidt, O. (2011b). Identity Construction Among Hackers. In K. Jaishankar (Ed.), *Cyber Criminology. Exploring internet Crimes and Criminal Behavior* (pp. 31-51). Boca Raton: CRC Press, Taylor & Francis Group.

UNODC. (2013). *Comprehensive study on cybercrime. Draft-February 2013*. New York: United Nations.

Van Beveren, J. (2001). A conceptual model of hacker development and motivation. *Journal of E-Business*, *1*(2), 1-9.

Van Der Broek, T.C., Van der Laan, A.M. & Weijters, G. (2016). Bedreiging via internet: Verschillen in risicofactoren tussen jongeren die online en offline bedreigen. *Panopticon, tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, *37*(2), 90-105.

Van Der Laan, A.M. & Goudriaan, G. (2016). *Monitor Jeugdcriminaliteit: Ontwikkelingen in de jeugdcriminaliteit 1997 tot 2015*. The Hague: WODC & CBS.

Van Der Laan, A.M., Beerthuizen, M.G.C.J. & Weijters, G. (2016). Jeugdige daders van online-criminaliteit. *Cahier Politiestudies*, *41*, 145-168.

Van Der Wagen, W. & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, 55, 578-595.

Van Der Wagen, W., Althoff, M. & Swaaningen, R. (2016). De andere 'anderen': Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur & Criminaliteit*, *6*(1), 27-41.

Van Eeten, M., Bauer, J.M., Asghare, H., Tabatabaie, S. & Rand, D. (2010). The Role of internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. STI Working paper 2010/5. Retrieved February 23, 2017, from: http://www.oecd.org/sti//.

Van Wilsem, J. (2011). "Bought it, but never got it": Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168-178.
Van Wilsem, J. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29, 437-453.
Veenstra, S., Zuurveen, R. & Stol, W.P. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland*. Leeuwarden: Lectoraat Cybersafety.
Voiskounsky, A.E. & Smyslova, O.V. (2003). Flow-based model of computer hackers' motivation. *CyberPsychology & behavior*, *6*(2), 171-180.
Wall, D.S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge: Polity Press.
Wall, D.S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107-124.
Wehinger, F. (2011). The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services. *Intelligence and Security Informatics Conference*. 10.1109/EISIC.2011.54.
West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34-40.
Willison, R. (2006). Understanding the offender/environment dynamic for computer crimes. *Information Technology & People*, *19*(2), 170-186.
WODC (2011). *Monitor Criminaliteit Bedrijfsleven 2010: Feiten en trends inzake aard en omvang van criminaliteit in het bedrijfsleven*. The Hague: WODC.
Woo, H.J. (2003). *The hacker mentality: exploring the relationship between psychological variables and hacking activities*. The University of Georgia, Athens, Georgia.
Xu, Z., Hu, Q. & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64-74.
Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387-399.
Yip, M., Shadbolt, N. & Webber, C. (2012). Structural Analysis of Online Criminal Social Networks. *IEEE International Conference on Intelligence and Security Informatics (ISI)*, 60-65.
Yip, M., Webber, C. & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & Society*, *23*(4), 516-539.
Young, R., Zhang, L. & Prybutok, V.R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281-287.
Zebel, S., De Vries, P., Giebels, E., Kuttschreuter, M. & Stol, W.P. (2014). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*. Twente: University of Twente, NHL, Police Academy of the Netherlands, Open University.

ANNEX 1: AUTHORS

EDITOR

Rutger Leukfeldt, postdoc researcher Cybercrime, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR).

AUTHORS

Below all the authors who contributed to this research agenda are listed in alphabetic order. Some others contributed to one specific topic of this research agenda while others worked on multiple topics. At the first page of each chapter, the authors who worked on that chapter are listed.

Jurjen Jansen, PhD candidate Open University of the Netherlands, researcher Cybersafety Research Group NHL, University of Applied Sciences and Police Academy of the Netherlands.

Floor Jansen, advisor, Team High Tech Crime of the Dutch National Police.

Marianne Junger, professor of Cyber Security, University of Twente.

Edward Kleemans, professor of Serious and Organized Crime and Criminal Justice, VU School of Criminologie, Vrije Universiteit Amsterdam, The Netherlands.

Bert-Jaap Koops, professor of Regulation and Technology, Tilburg University.

Joke Kort, researcher and consultant TNO, Expertise Group for Human Behaviour and Organizational Innovation.

André van der Laan, senior researcher and deputy head of the Crime, Law Enforcement and Sanctions Division of the Research and Documentation Centre (WODC), Ministry of Security and Justice.

Anita Lavorgna, researcher Organized Crime, University of Southampton.

Jarmo van Lenthe, digital crime investigator, Team High Tech Crime of the Dutch National Police.

Rutger Leukfeldt, postdoc researcher Cybercrime, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR).

Eva Maas, policy officer, DNB (Dutch Central Bank) (former policy officer at the Ministry of Security and Justice).

Erik Planken, senior policy advisor, Ministry of Security and Justice.

Christianne de Poot, professor of Criminalistics Vrije Universiteit Amsterdam, senior researcher at the Research and Documentation Centre (WODC), Ministry of Security and Justice, head of the Forensic Research Department Amsterdam University of Applied Sciences.

Bart Schermer, associate professor of eLaw, Leiden University, Partner at Considerati.

Wouter Stol, professor of Police Studies Open University of the Netherlands. Head of the Cyber Safety Research Group

NHL University of Applied Sciences and Police Academy of the Netherlands.

Sander Veenstra, researcher Cyber Safety Research Group NHL University of Applied Sciences and Police Academy of the Netherlands.

Maite Verhoeven, researcher Research and Documentation Centre (WODC), Ministry of Security and Justice.

Wytske van der Wagen, PhD candidate University of Groningen, researcher Erasmus University Rotterdam.

Gijs Weijters, researcher Research and Documentation Centre (WODC), Ministry of Security and Justice.

Marleen Weulen Kranenbarg, PhD candidate Netherlands Institute for the Study of Crime and Law Enforcement.

Johan van Wilsem, Director Research Department Crime, Law Enforcement and sanction of the Research and Documentation Centre (WODC), Ministry of Security and Justice (former associate professor Leiden University).

Sophie van der Zee, researcher Vrije Universiteit Amsterdam (former researcher and consultant TNO).

ANNEX 2: PARTICIPANTS DISCUSSION SESSIONS

Christaan Baardman, senior counselor and director, Cybercrime Centre, The Hague Court.

Catrien Bijleveld, professor of Research Methods in Criminology, VU University, Amsterdam, director of the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR).

Jarno van Boven, advisor, police department Northern Netherlands.

Carlijn Broekman, consultant on co-creation and new media, TNO.

Marjolein Faassen, lecturer, The Hague University of Applied Sciences.

Tamar Fisher, associate professor, Erasmus University Rotterdam.

Marit van Galen, advisor, Dutch National Cyber Security Center.

Heike Goudriaan, senior statistical researcher, Statistics Netherlands.

René Hesseling, senior researcher, Police Department The Hague.

Anne de Hingh, associate professor, VU University, Amsterdam.

Arjan de Jong, advisor, Dutch National Cyber Security Center.

Godfried Klerkx, advisor, Dutch National Police, Cybercrime Program (PIAC).

Arianne Kuik-Knoesteren, lecturer, The Hague University of Applied Sciences.

Arno Lodder, professor of internet Governance and Regulation, VU University, Amsterdam

Annemarie van der Meer, advisor, police department, Northern Netherlands.

Elke Moons, statistical researcher on safety, Statistics Netherlands.

Jan Jaap Oerlemans, researcher, WODC.

Kim Oosterwijk, junior researcher, Erasmus University Rotterdam.

Wolter Pieters, assistant professor of Cyber Risk, Delft University of Technology.

Stijn Ruiter, professor of Social and Spatial Aspects of Deviant Behavior, Utrecht University, senior researcher Netherlands Institute for the Study of Crime and Law Enforcement (NSCR).

Lisanne Slot, project manager, Cyber Security in SMEs, Centre of Expertise Cyber Security, The Hague University of Applied Sciences.

Marcel Smetsers, policy advisor high tech crime, National Prosecutor.

Jelle van Triest, policy advisor, Dutch Probation Service.

Frank Weerman, professor of Youth Criminology, Erasmus University Rotterdam, Senior Researcher Netherlands Institute for the Study of Crime and Law Enforcement (NSCR).