Global voices in hacking (multinational views)

Weulen Kranenbarg, Marleen

published in
The Palgrave Handbook of International Cybercrime and Cyberdeviance
2020

DOI (link to publisher)
10.1007/978-3-319-78440-3_33

document version
Publisher's PDF, also known as Version of record

document license
Article 25fa Dutch Copyright Act

Global Voices in Hacking (Multinational Views)

37

Marleen Weulen Kranenbarg

Contents

Introduction 772
Judicial Population Research 773
Quantitative Survey Research 773
Personal Characteristics and Situational Risk Factors 774
Social Networks 776
Specialization and Motives 776
Qualitative Interview Research 777
Labelling 777
Cyborg Hackers 778
Research Based on Police Records and Files 780
Quantitative Life-Course Research 780
Qualitative Research on Organized Cybercrime 781
Concluding Remarks on Studying Hackers with Judicial Population Research 783
General Populations Research 783
Conclusion and Discussion 785
Cross-References 786
References 787

Abstract

This chapter will give an overview of research on hacking in the Netherlands and other non-English-language countries. Findings from these countries will be compared to general findings in the literature. The chapter will start with both qualitative and quantitative research based on judicial populations. These studies address topics like personal characteristics and situational risk factors of hackers, their social networks, their specialization and motives, labelling, the extent to

M. Weulen Kranenbarg (✉)
Vrije Universiteit (VU) Amsterdam, Amsterdam, The Netherlands
e-mail: M.WeulenKranenbarg@vu.nl

T. J. Holt, A. M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_33

which hackers can be seen as cyborg hackers, life-course research, and the role of hackers in organized cybercrime. Afterward, survey research on cyber-dependent offending among youth, based on general population samples, will be discussed. The chapter ends with a discussion on the need of international comparative research on hackers.

Keywords

Hacking · System trespassing · Cyber-dependent offenders · International · Comparison · Samples · Quantitative · Qualitative

Introduction

The majority of the English-language literature on hackers is based on research from English-speaking countries. These studies provide valuable insight into hackers, their characteristics, modus operandi, and networks. However, this English-language sample frame also limits the generalizability of these studies and the different types of methods used. This chapter will, therefore, discuss research from non-English-language countries, with a specific focus on hacking research from the Netherlands. In addition to this focus, it will discuss research published in English that originates from other non-English countries, as these can provide unique perspectives on hacking, other samples or methodologies, or cross-country comparisons. Where possible, the results from these studies will be compared to general findings in the literature.

There are several reasons why Dutch research on hacking can provide valuable insights. Calculations by Internet Live Stats (2018) show that in 2016 93.7% of the Dutch population had access to the Internet at home. This means that the Netherlands is in the top ten of countries with the highest Internet penetration rate, above the United Kingdom and the United States. This results in high opportunities for crime and risks for victimization. This is reflected in the Dutch nationally representative victimization surveys, which have shown a remarkable trend in hacking victimization. While bicycle theft has long been the most common type of victimization in the Netherlands, hacking is now more prevalent. While in 2017 only 3.3% of the population had their bicycle stolen, 4.9% of the population was victimized by hacking (Statistics Netherlands 2018).

With respect to research on hackers, Dutch studies have been using unique data sources and methodologies. While quite some international hacking literature focuses on forum data from, for example, English or Russian language forums (see, e.g., Dupont et al. 2016; Holt 2013; Holt et al. 2012b, 2016a, b; Macdonald and Frank 2017), there are no well-known and large-scale Dutch forums. Therefore, Dutch research tends to focus on other types of data. In general, two types of samples are used. First, collaborations with the police and prosecutor's office provide opportunities to interview or survey known offenders (Van Der Wagen 2018a; Van Der Wagen et al. 2016; Weulen Kranenbarg 2018; Weulen Kranenbarg et al. 2019). These collaborations also allow for qualitative and quantitative research using police records. The growing focus on cybercrime in the police force will continue

to provide this type of valuable information on criminal hackers. Second, the size of the country allows for surveying representative general population samples, usually focused on youth (Rokven et al. 2017b; Van Der Laan and Beerthuizen 2018; Van Der Laan and Goudriaan 2016).

The developments above recently resulted in more attention toward human factor research on cybercrime in the Netherlands. One of the results of this development is a research agenda on *The Human Factor in Cybercrime and Cybersecurity*, which also includes a chapter on individual offenders (Weulen Kranenbarg et al. 2017) and cybercriminal networks (Leukfeldt et al. 2017). This state of the art of the literature was not specifically focused on Dutch hacking research and also included research on other types of cyber-offending and research from other (mostly English-language) countries. Since the publication of this research agenda, new and innovative Dutch research on hackers has been published, which will be the focus of this chapter in relation to the more general findings in the hacking literature.

This chapter will start with discussing both quantitative and qualitative research based on judicial populations and police files. The nature of these samples, and the associated permissions that are required to use these, means that these studies are mostly focused on adult hackers (Van Der Wagen 2018a; Van Der Wagen et al. 2016; Weulen Kranenbarg 2018; Weulen Kranenbarg et al. 2019). Afterward, the chapter will focus on self-report general population studies, which are usually focused on youth (Rokven et al. 2017b; Van Der Laan and Beerthuizen 2018; Van Der Laan and Goudriaan 2016). Throughout the chapter, studies from other non-English countries will be discussed as well, and findings will be discussed in the light of findings in the general hacking literature. In the conclusion and discussion, the need for international comparative research will be discussed.

Judicial Population Research

There are basically two ways in which specifically Dutch research uses judicial information on known criminal hackers: first, by quantitatively surveying (Weulen Kranenbarg 2018; Weulen Kranenbarg et al. 2019) or qualitatively interviewing (Van Der Wagen 2018a; Van Der Wagen et al. 2016) individuals who have been in contact with the judicial system for criminal hacking and, second, by conducting research on police records, which can be both quantitative research on the full judicial population (Ruiter and Bernaards 2013; Weulen Kranenbarg et al. 2018b) and qualitative case studies based on police files (Van Der Wagen 2018a; Van Der Wagen et al. 2016). Some studies also combine these methods (Van Der Wagen 2018a; Van Der Wagen et al. 2016).

Quantitative Survey Research

Weulen Kranenbarg (2018) used a survey among a sample of 535 known offenders registered by the Dutch public prosecutor's office. Half of this sample had been suspected of committing a traditional crime; the other half had been suspected of

committing a cyber-dependent crime. The cyber-dependent crimes in this study (in order of prevalence) were guessing passwords, defacing, digital theft, other types of hacking, damaging data, taking control over an IT system, phishing, malware use, intercepting communication, DoS attacks, selling somebody else's data, spamming, and selling somebody else's credentials (for prevalence rates, see Weulen Kranenbarg 2018; Weulen Kranenbarg et al. 2019). These are almost all crimes that require some form of hacking. The goal of this study was to examine these offenders' personal characteristics and situational risk factors, their social networks, the extent to which they specialize or also commit traditional offenses, and their motives for offending. In addition, the goal was to compare the cyber-dependent offenders on these aspects with traditional offenders. However, in this chapter the focus will be on the findings for the cyber-dependent offenders. Detailed information on the survey-based comparison can be found in Weulen Kranenbarg (2018) and Weulen Kranenbarg et al. (2019).

A unique feature of this survey study was the inclusion of an objective information technology (IT) skills test. Several cybercrime studies (e.g., Holt et al. 2010; Lee 2018) use a subjective IT skills survey question based on Holt et al. (2012a, p. 389), in which respondents are asked to indicate which of the following statements applies to their IT skills: "I am afraid of computers and don't use them unless I absolutely have to," "I can surf the net, use common software, but cannot fix my own computer," "I can use a variety of software and fix some computer problems I have," and "I can use Linux, most software, and fix most computer problems I have." As Weulen Kranenbarg (2018) used a sample in which IT skills of some offenders were expected to be very strong, an additional statement was added to these four statements: "I can use different programming languages and am capable of detecting programming errors." More importantly, the survey included ten multiple-choice test questions. These varied from very easy questions on, for example, what a valid email address looks like, which was answered correctly by 92.49% of the sample, to very challenging questions in which respondents had to find a coding error and come up with a way to prevent misuse of that error, which was only answered correctly by 4.34% of the sample. This objective IT skills measure is an interesting additional way of measuring IT skills, which showed a strong correlation with the subjective IT skills measure with the five statements discussed above.

Personal Characteristics and Situational Risk Factors

In the international literature, one consistent correlate of both traditional offending (Berg and Felson 2016; Jennings et al. 2012; Lauritsen and Laub 2007) and cyber-offending (in both English and non-English research; see, e.g., Bossler and Holt 2009; Kerstens and Jansen 2016; Morris 2011; Ngo and Paternoster 2011; Wolfe et al. 2008) is that offenders are often also victims. One of the explanations is that offenders and victims share characteristics like low self-control and risky daily activities that increase both their risk for offending and victimization. In line with this general picture in the literature, a Dutch study on a large youth sample also

found this victim-offender overlap for online auction fraud, virtual theft, and online identity fraud (Kerstens and Jansen 2016). Subsequently, Weulen Kranenbarg et al. (2019) showed that this overlap can also be found in a sample of known Dutch cyber-dependent offenders, as 9.59% of the sample reported both to have committed a cyber-dependent crime and have been victimized by a cyber-dependent crime in the preceding 12 months. In addition, 8.06% of the sample committed a cyber-dependent crime without being victimized. Further examination of these two groups revealed that it is important to study their characteristics separately, something that has not yet been done in the aforementioned international literature on hacking.

The offenders that had not been victimized appeared to have committed the more sophisticated types of cybercrime (Weulen Kranenbarg et al. 2019). The analyses of their characteristics also revealed that they were the group of offenders with very specific characteristics that clearly distinguish them from traditional offenders. For example, they did not have statistically significant low self-control; they had strong IT skills and specific situational risk factors like spending a lot of time on forums where they can learn more on how to commit these more sophisticated types of crime. It appears that these characteristics provide them with the opportunities to commit these offenses and the ability to prevent themselves from being victimized. On the other hand, the offenders who were also victimized committed the less sophisticated types of cybercrime and showed a more general risk profile. Apart from their online situational risk factors, they were more comparable to traditional victim-offenders. These cyber-dependent victim-offenders had low self-control, some IT skills (but less than the first group), and more general online activities in which both their opportunities for easy-to-commit cybercrime and their risks for being victimized were increased. In line with the explanation that offenders and victims share risk factors, the characteristics of the victim-offenders like low self-control seem to increase their risk-taking behavior, which is related to both offending and victimization. IT skills of victim-offenders were, apparently, not strong enough to prevent their victimization.

In short, this study revealed that different correlates can be found when looking at different types of hacking (Weulen Kranenbarg et al. 2019). Similar findings can be found in the international literature. For example, while some studies find that hacking or other cybercrimes are related to low self-control (Donner et al. 2014; Hu et al. 2013; Marcum et al. 2014), others find that the effect of self-control differs in relation to IT knowledge and the extent to which social learning plays a role (Bossler and Burruss 2011; Holt et al. 2012a). With respect to learning of skills, forums and other online networks have also been found to be an important source of information (Holt 2007; Holt et al. 2012b; Hutchings 2014; Hutchings and Clayton 2016), which explains the correlation between forum use and more sophisticated types of offending (Weulen Kranenbarg et al. 2019). In the light of these results, it should also be noted that there is some international research on the extent to which autism traits are related to hacking (Harvey et al. 2016; National Crime Agency 2017; Schell and Melnychuk 2011). However, while it makes sense to assume that some autism traits are related to hacking, there is no strong evidence for this claim yet.

Social Networks

As already briefly mentioned above, many studies that mostly originate from English-language countries have indicated that having delinquent peers is an important correlate of hacking (Bossler and Burruss 2011; Donner et al. 2014; Holt 2007; Holt et al. 2010, 2012a; Holt and Kilger 2008; Hu et al. 2013; Marcum et al. 2014; Morris 2011; Morris and Blackburn 2009; Rogers 2001). These studies are, however, mostly based on student or school samples. In line with this international literature, the Dutch judicial population research of Weulen Kranenbarg et al. (2019) also found this relationship between offending and deviance of social contacts, even when controlling for other characteristics that are similar among social contacts like gender and age. Controlling for similar characteristics was enabled by the type of network data collected in this study, which had not yet been done in the international literature mentioned above. An even more important addition to the international literature, however, were the findings from the comparison with traditional offenders. This revealed that the relationship between offending and deviance of social contacts is much weaker for cyber-dependent crime, compared to traditional crime.

Weulen Kranenbarg et al. (2019) specifically focused on important social ties, with whom offenders discuss important matters. These social contacts traditionally have the strongest impact on offending (Rokven et al. 2016, 2017a). The fact that their deviance is less strongly correlated to cyber-dependent offending can be explained in two ways. First, it could be the case that cyber-dependent offenders have more loose online social ties. Second, it could be that cyber-dependent offenders are more on their own and less inclined to seek close contact with others. The Internet could also provide a source of information on how to commit these offenses without having to have contact with others (Goldsmith and Brewer 2015; Weulen Kranenbarg et al. 2019). At the moment, it is unclear to what extent the possible explanations above are valid. In general, Weulen Kranenbarg et al. (2019) showed that research on cyber-dependent offenders should broaden its perspective to other types of social contacts. Forums, for example, could be a new place for social learning and social interactions but may also influence someone's behavior in a completely different way than traditional offline social interactions. As stated in the introduction, it should be noted that there are no well-known Dutch hacking forums. Therefore, existing Dutch forum research has focused on interaction on English-language forums (Soudijn and Zegers 2012), similar to the aforementioned general literature on hacking forums (Dupont et al. 2016; Holt et al. 2012b; Macdonald and Frank 2017). Planned future longitudinal research will distinguish between online and offline social contacts and the extent to which both influence and selection processes underlie the correlation between offending of peers.

Specialization and Motives

Lastly, the self-report data from the judicial population survey has been used to examine to what extent specialization occurs in cyber-dependent crime and which motives offenders report for committing these offenses (Weulen Kranenbarg 2018). With respect to specialization, in this sample most offenders do not combine cyber-dependent

offenses with traditional offenses. In addition, within the group of cyber-dependent offenders, some forms of specialization can be found. Hacking is generally seen as a first step in an offender's modus operandi (Leukfeldt et al. 2013; Maimon and Louderback 2019). This was also indicated by Weulen Kranenbarg (2018), as offenders usually combined hacking with offenses like stealing or damaging data.

With respect to the motives for committing these offenses, this study indicated that most offenders commit their crimes for intrinsic motives like curiosity or the challenge of breaking systems. For some offenses, extrinsic motives like sending a message or revenge were also mentioned (Weulen Kranenbarg 2018). This is mostly in line with the early work of Jordan and Taylor (1998) and Taylor (1999), which included qualitative fieldwork of motives in the international hacker culture and other international research on motives (e.g., Chiesa et al. 2008; Denning 2011; Holt 2007, 2009; Voiskounsky and Smyslova 2003; Woo 2003). In the sample of Weulen Kranenbarg (2018), financial motives were almost completely absent. This is striking, as the reported motives for traditional offenses were often financial. In addition, it is interesting as some argue that all cybercrime is now financially motivated (Chan and Wang 2015; Grabosky 2017; Holt and Kilger 2012; Kshetri 2009; Provos et al. 2009; Smith 2015; White 2013). In line with those arguments, it should be noted that a German self-report study found strong financial motives for identity theft-related types of hacking (Fotinger and Ziegler 2004). These similarities and differences between studies indicate that different samples may result in very different motives for committing these offenses. As some studies use motives in addition to characteristics like organization, resources, expertise, and target to develop threat actor typologies (De Bruijne et al. 2017), it is important to find empirical evidence for these motives.

Qualitative Interview Research

Van der Wagen (2018a; Van Der Wagen et al. 2016) has conducted research on Dutch hackers by using different methodologies, including qualitative interviews and analyzing police files. The interviews are with hackers in general, both the ones that commit crimes and the ones that try to improve cybersecurity. In Van Der Wagen et al. (2016), ten qualitative in-depth interviews with hackers are used to explore processes of labelling in the hacker community. Nine of these hackers had the Dutch nationality, and half of them considered themselves to be white hat or ethical hackers, while the other half had been involved with black hat hacking. Thus, sampling was not specifically based on offenders who had been in contact with the judicial system. However, these interviews were complemented with information from five police files on hacking cases.

Labelling

In Van Der Wagen et al. (2016), three dimensions of the deviant identity were examined: the way in which hackers perceive that other "normal people" see them, the way in which they see themselves and their actions, and the way in which

as outsiders they see themselves in relation to the conventional society and in relation to other outsiders. The interviewed hackers experience negative labelling effects. They feel that "normal people" have a negative image of them. Nevertheless, their perception of their own identity is positive. They feel like they have a special gift, which offers them more opportunities than others have. The online community offers positive reinforcement of their actions, which reduces the negative effect of the offline conventional society. Therefore, Van Der Wagen et al. (2016) conclude that the negative labelling does not result in stigmatization of these hackers. In addition, with respect to how they see themselves in comparison to other outsiders, these hackers, both white hat and black hat, all agree that they are not real cybercriminals. In line with the research discussed above, only one of the black hat hackers indicated that he had hacked for financial gain. All respondents in this research said that hacking is only criminal if the offender has financial motives. This was also clear in some of the studied police files with hacking cases.

Labelling has been almost completely absent in the international literature on hacking. Similar findings on this topic can, however, be found in research from a different non-English country. The earlier work of Turgeman-Goldschmidt (2005, 2008, 2009, 2011a, b) is based on 54 interviews with Israeli hackers. This research also indicated that hackers experience negative labelling by others, but they see themselves as positive deviants (Turgeman-Goldschmidt 2008, 2011b). In addition, they also differ from other deviants in their use of neutralization techniques (Turgeman-Goldschmidt 2009). They do not use external justifications for their behavior. They only use internal justifications like denial of injury, denial of victim, condemnation of the condemners, appeal to higher loyalties, and self-fulfillment. These neutralizations techniques are also in line with the labelling processes described in Van Der Wagen et al. (2016) and Turgeman-Goldschmidt (2008) and other international research on neutralization among hackers (e.g., Chua and Holt 2016; Hutchings and Clayton 2016; Morris 2011; Young et al. 2007). Again, the hackers in Turgeman-Goldschmidt (2005) also did not commit their crimes for financial gain. Their hacking can be seen as a form of social entertainment. Turgeman-Goldschmidt (2011a) further argues that the absence of a financial motive and absence of external justifications mean that hackers cannot be considered white-collar offenders, even though they do have some similar characteristics. Similarities and differences between cyber-offenders and white-collar offenders have also been found in cases from the United States (Pontell and Rosoff 2009).

Cyborg Hackers

The main theme in the research of Van der Wagen is the cyborg perspective based on the actor-network theory (Latour 1992, 2005). In this line of research, Van Der Wagen (2018b) examines to what extent the relationship between humans and technology should be part of our understanding of cybercriminal behavior. Almost all international criminological research discussed in this chapter focuses on the human and looks at technology only as an instrument to commit cybercrimes.

In this research, on the other hand, technology is considered an active and vital part that interacts with the human actor. This perspective has been used to study different aspects of cybercrime, including botnets (Van Der Wagen and Pieters 2015), cybercriminal networks (Van Der Wagen and Bernaards 2018), victims (Van Der Wagen and Pieters 2018), and hackers (Van Der Wagen 2018a), by using both interview data and police files. As this chapter is on hackers, it will focus on the extent to which hackers can be considered to be cyborgian deviants and how hackers view their relationship with technology.

The ten interviews with both white hat and black hat hackers indicated that both for the process of becoming a hacker and being a hacker, the relationship of the hacker with the technology is a vital component. Van Der Wagen (2018a) states that hackers and technology should not be seen as two completely different things. Hackers interact with technology in different ways. They work with technology, they act through technology, and they sometimes act against technology. In these interactions, they look for the boundaries of technology and see to what extent they can overcome these boundaries, which could but does not have to result in committing crime. This notion of boundaries can also be found in the Israeli work of Turgeman-Goldschmidt (2005) and the ethnographic US-based research from Steinmetz (2015).

Based on the interviews, Van Der Wagen (2018a) describes five dimensions of the relationship between hackers and technology: mind, performance, identity, body, and transgression. With respect to the *mind*, hackers are interested in the underlying processes of systems. They have an analytical perspective and want to fully understand a system, so that they can use it in innovative ways and completely control them. In their perspective, systems are more than just a static tool (Van Der Wagen 2018a). The botnet police file case study (Van Der Wagen and Pieters 2015) also revealed that by using hacking techniques, a hacker can also make a system work for him. By hacking into websites, the hacker was able to automatically spread malware, which in turn added new computers to the botnet.

In line with the arguments about learning from other sources than strong social ties provided earlier (Goldsmith and Brewer 2015; Weulen Kranenbarg et al. 2019), hackers describe that they also learn by trial and error in interaction with systems (Van Der Wagen 2018a). Their *performance* is, however, not only the result of their own capabilities but also of the capabilities of the system that they use. The hackers describe their *identity* as having a natural or innate connection with technology and an ability to see things other people do not see, which provides them with the abilities and drive to keep learning about systems. Hackers rely on their *body* (mostly their brain) to respond intuitively on technological challenges. That is also why they keep challenging their own capabilities and technical capabilities. Lastly, with respect to *transgression*, the euphoric feeling after a successful hack challenges even the white hat hackers. The world of possibilities when one has finally gained access to a system may be too tempting which could result in misuse of the system (Van Der Wagen 2018a). Although only Van Der Wagen specifically applied the actor-network theory to this relationship between hackers and technology, other international studies have found similar characteristics of hacker culture (e.g., Steinmetz 2015; Taylor 1999; see ► Chap. 35, "Computer Hacking and the Hacker Subculture").

Research Based on Police Records and Files

In the research of Van der Wagen described above, police files have been used as case studies, mostly to enrich interview data. However, there is a long tradition of collaborations between researchers and police forces in the Netherlands, which enables Dutch criminologists to use police records and files as their main source of data as well. Police records provide limited but full offender population data, which is usually analyzed in a quantitative manner. Police files, on the other hand, provide in-depth data on specific cases that are usually studied in a qualitative manner. This section will first discuss two quantitative longitudinal life-course studies based on police records (Ruiter and Bernaards 2013; Weulen Kranenbarg 2018). Afterward, it will discuss some qualitative studies on police files (Bijlenga and Kleemans 2018; Bulanova-Hristova et al. 2016; Kruisbergen et al. 2018b; Leukfeldt et al. 2017a, b, c, d; Odinot et al. 2017, 2018).

Quantitative Life-Course Research

A first longitudinal study on the life course of hackers has been conducted by Ruiter and Bernaards (2013). In this study a group of 323 hackers who had been registered as a suspect in the Dutch police registration system have been compared to other suspects on their sociodemographic characteristics and age-crime curves. The analyses indicated no differences in ethnicity and gender. To the same extent as other suspects, some registered criminal hackers already had a criminal record, or they committed other crimes after their registration for hacking. Recidivism in hacking could not be found in these data. However, as these are only the crimes that the police know about, it is likely that recidivism did take place. This is also confirmed by the survey of Weulen Kranenbarg (2018), in which a proportion of the hackers who had been in contact with the police self-reported recidivism in hacking. Even though the data of Ruiter and Bernaards (2013) have limitations, the longitudinal comparison of criminal careers of hackers with other offenders provides a unique perspective. The analyses showed that the criminal careers of hackers, as registered by the police, follow a similar pattern in age-crime curve, onset, and persistence as other criminals.

This first study could only examine some basic sociodemographic characteristics. This means that it could not examine which life circumstances are related to a person's offending or desistence. Weulen Kranenbarg et al. (2018b) combined the police registration data for all adult suspects ($N = 870$ cyber-dependent suspects and $N = 1{,}144{,}740$ other suspects) with other registration data from Statistics Netherlands for the period of 2000–2012. This enabled a longitudinal within-person examination of the relation between living with a partner or family, being employed, and being enrolled in education. In these within-person analyses, the years in which a person, for example, is employed are compared with the years in which that same person is unemployed, to see in which years that person is more likely to commit a cyber-dependent offense. In this research, there is a distinction between employment

and education in de IT sector and general employment or education. The authors provide several augments why these traditionally important preventive life circumstances may not have the same effect on cyber-dependent offending.

In contrast to these arguments, with respect to the effect of a partner or family, cyber-dependent offenders are similar to other offenders as they are less likely to offend in years in which they live together with a partner or a family (partner and child) compared to the years in which they live alone. For all types of crime, including cyber-dependent crime, living as a single parent can increase offending. With respect to employment and education, on the other hand, the results were in line with the expectations. In general being employed had a preventive effect on cyber-dependent offending in this full suspect population. More importantly, however, people were more likely to commit cyber-dependent offenses in years in which they were employed in the IT sector or enrolled in education in general. This indicates that indirect social control of family can prevent cyber-dependent offending, but opportunities for these offenses occur in very different environments than opportunities for other crimes. Some life circumstances like specific types of employment can create these opportunities, and social control in those situations is not strong enough to prevent offending (Weulen Kranenbarg et al. 2018b). This can also be found in the international literature, where surveying American hackers on a hacker convention revealed that they have less strong social ties and more time to hack when they are unemployed (Bachmann 2010). On the other hand, other studies that focus on insiders have also indicated that cybercrimes can be employment-enabled (Grabosky and Walkley 2007; Nykodym et al. 2005; Randazzo et al. 2005). It seems that it will depend on the type of employment and opportunities, if employment is a protective factor or a risk factor.

Qualitative Research on Organized Cybercrime

The quantitative research based on police records discussed above is unique in the sense that it provides longitudinal information on the full population of suspects registered by the police. However, the nature of the data does not allow for very detailed and in-depth analyses on each specific case. In qualitative case studies based on police files, on the other hand, the goal is not to present an overall representative picture of these cases but to provide a more in-depth understanding of these cases. This information is very valuable on itself but also in combination with research based on other methodologies. For example, Bijlenga and Kleemans (2018) analyzed five criminal investigations and found that some organized crime groups specifically contact employees in the IT sector to help them with parts of their crime script that require IT expertise, which is in line with the life-course research discussed above (Weulen Kranenbarg et al. 2018b). In the Netherlands this type of research by using police files has mainly been used to study organized crime in the so-called Organized Crime Monitor (see Research and Documentation Center 2018). In recent years, cybercrime cases have been added to this data collection. This is a very wide range of types of cybercrime cases, from online drug trade to advanced

banking malware cases. This chapter will focus on the results about hackers in these cases. For a broader English summary of recent results about organized crime and IT in the Netherlands, see Kruisbergen et al. (2018b, pp. 109–118).

At the moment, seven cybercrime cases have been analyzed as part of the Organized Crime Monitor. However, other studies have analyzed numerous additional cases. In general, if there are hackers involved in these cases, they mainly act as facilitators. For example, the most well-known case is probably a drug trafficking case, in which two hackers were used by the organization to hack into the systems of the port, so that their container with drugs could enter the Netherlands undetected. In addition, in two cases malware writers wrote banking malware that was used to take over the IT systems of the victims to manipulate their online transactions (Kruisbergen et al. 2018b). In these cases, criminal networks that largely exist offline may use forums to find these malware writers (Leukfeldt et al. 2017a). The rest of the members of these networks do not have very strong IT skills. This shows how international research on these forums and the social organization of online cybercriminal services (Dupont et al. 2016; Holt 2013; Holt et al. 2012b, 2016a, b; Hutchings 2014; Hutchings and Clayton 2016; Macdonald and Frank 2017) can be very relevant even when studying a domestic and largely offline case.

In contrast to research on individual hackers discussed earlier in this chapter (Denning 2011; Holt 2007, 2009; Turgeman-Goldschmidt 2005, 2008, 2011a; Van Der Wagen et al. 2016; Voiskounsky and Smyslova 2003; Weulen Kranenbarg 2018; Woo 2003), these organized crime studies tend to find financial motives for acting as a facilitating hacker in these networks (Kruisbergen et al. 2018b). This clearly stresses the importance of using different samples to study hackers. With respect to this financial motive, it is interesting to see that even if the crime script is a high-tech form of crime, the networks still show a need for cash (Kruisbergen et al. 2018a, b) and many networks still consist of groups of offenders who know each other offline (Leukfeldt et al. 2017c). This has not only been found in the Netherlands but in several other countries (Lusthaus 2018). A case study on Romania by Lusthaus and Varese (2017), for example, has also shown that cybercrime can have an important local and offline dimension.

The cases discussed above are part of research on organized crime in general. However, some case studies have specifically added more high-tech organized cybercrime cases to their analyses. Hackers often have a more central role in these cases; see, for example, Odinot et al. (2017). This report also discusses some background characteristics of the 39 members of the organized crime groups who commit the IT-related parts of the crime script. In these cases, they are younger than the other members of the group are (29 vs. 37 years). In line with Ruiter and Bernaards (2013) discussed earlier, nine had previous convictions, but only three were convicted for hacking. Although money was the main motive in these cases, some hackers had motives related to revenge or hacking being their hobby, and some were pressured or forced by others.

Lastly, a few studies have used these case files in international comparisons. The study discussed in the previous paragraph was part of a cross-national comparison between the Netherlands (11 cases), Sweden (15 cases), and Germany (18 cases)

(Bulanova-Hristova et al. 2016; Odinot et al. 2018). These comparisons seem to confirm the overall picture on Dutch cases. Some important findings are that offenders in these networks tend to be younger than offenders in other organized crime networks. In addition, the possibilities of contacting hackers for a part of the crime script enable traditional organized crime groups to engage in forms of cybercrime as well. However, new groups that were not yet involved in organized crime also emerge in the field of organized cybercrime. In a similar manner, Leukfeldt et al. (2017b, d) compared Dutch results on the use of online crime markets and the origin, growth, and criminal capabilities of cybercriminal networks with cases from Germany and the United Kingdom. It should be noted, however, that the selective and nonrepresentative nature of this type of data makes international comparisons difficult.

Concluding Remarks on Studying Hackers with Judicial Population Research

As shown above, judicial populations provide unique ways to study hacking or cybercrime in general. However, in these studies, it is not always clear how technical this type of hacking is, and many studies include a very broad range of cyber-offenses including hacking. Research on police files has shown that hacking is often only a small part or starting point of the crime (Leukfeldt et al. 2013). Hacking cases generally only have few suspects, which means that these cases will not be studied in organized crime research as discussed above. In addition, this research showed that in many case files on hacking, crucial information about the way in which the suspect hacked into a system is missing. As hacking can be done by simply guessing a password, not all suspects registered as hackers will have the technical capabilities that we generally associate with hackers. Lastly, of course, the hackers that are caught may be the ones that are less capable of hiding their crime, which may mean that research based on these hackers underestimates the skills of the general criminal hacker population. However, as indicated by Weulen Kranenbarg et al. (2019), more sophisticated types of hacking do emerge in these samples, which are also reflected in the IT skills of those offenders. This may be the result of police forces that are specifically targeting high-tech cybercrime.

General Populations Research

In order to gain more insight into hacking in the general population, it is important to review survey research that is focused on general population samples. The advantage of using these samples is that the results are more representative than the results discussed above. However, it should also be noted that these results generally do not primarily focus on high-tech forms of hacking, as these offenses are not prevalent enough in the general population. Nevertheless, as Dutch research in this area focuses on youth, this does provide information that cannot be found in the judicial

population research discussed above. In the Netherlands this type of data is collected in the Juvenile Crime Monitor and is combined with data from police records in a biennial report (Van Der Laan and Beerthuizen 2018). In 2015 the most recent self-report study has been conducted, published in the 2016 report (Van Der Laan and Goudriaan 2016).

The reports above are mostly descriptive and provide information on all kinds of crime, including different types of cybercrime. The 2017 report presents an overall picture of the number of police records and convictions on cyber-dependent crimes (including hacking) for youth. The conclusion is that these numbers are very low, but that that must be a result of the data source as the 2016 report that includes self-report data shows much higher numbers (Van Der Laan and Beerthuizen 2018; Van Der Laan and Goudriaan 2016). Because of these limitations, new ways of extracting quantifiable data from police files and new types of prevalence research among youth are being explored (see, e.g., Van Der Heijden et al. 2017).

The 2016 results based on the self-report data paint the following picture about the five cyber-dependent offenses included (changing someone's password, hacking, i.e., logging in to someone else's computer/account, hacking including altering data, spreading a virus, DDoS attack). Young adults are relatively more involved in these offenses than children are (22% age 18–23; 17% age 12–17; 7% age <12). Especially hacking shows this trend of increasing by age (18% age 18–23; 12% age 12–17; 6% age <12), which the authors explain by suggesting that this requires some skills that need to be learned. It is also striking that among the young adults, these cyber-dependent offenses together with offline property crimes are more common than all other offline or online offenses. Nevertheless, the report concludes that the lack of longitudinal data on cyber-dependent offenses makes it impossible to test to what extent youth change their offending behavior from offline to online crime. A last interesting finding of this study is that, in contrast to, for example, police data on adult hackers (Ruiter and Bernaards 2013; Weulen Kranenbarg et al. 2018b) or cybercrime cases in the United Kingdom (Hutchings and Chua 2016), self-report data from youth between 12 and 23 years old shows that cyber-dependent offending is quite evenly distributed among boys and girls. It should be noted that the crimes included are quite broadly defined and can also include types of behavior that one may not see as crime, while offenses like using ransomware are missing (Beerthuizen et al. 2017).

Rokven et al. (2017b) tried to answer the question of whether offending among youth shifts to the online world, something that is often assumed in the international literature. They used the self-report data on 12–23-year-olds discussed above. It should be noted that, based on factor analyses, pretending to be someone else online is also part of the group of cyber-dependent offenses, in addition to the offenses above. By combining this data with other data on these youth, this study moved beyond the descriptive nature of the research discussed above, by analyzing the profiles of self-reported delinquents. In these profiles, the report distinguishes between youth who only commit cyber-enabled offenses, youth who only commit cyber-dependent offenses, and youth who commit both. In this chapter, the results that distinguish cyber-dependent only offenders from the other two groups will be

discussed. The English summary of the report (Rokven et al. 2017b) and the publication by Rokven et al. (2018) include the other profiles.

For 12–17-year-olds, profiles of cyber-dependent offenders clearly differ from the profiles of cyber-enabled offenders. They are more often involved in gaming and tend to disapprove of offline offending more. They are also more open toward their parents and have fewer cyber-enabled delinquent friends. For 18–23-year-olds, the cyber-dependent offenders have a less severe risk profile. Overall, their profiles show that they are less often victims of offline offenses; they have fewer offline delinquent friends and fewer cyber-enabled delinquent friends. With respect to comparing with profiles of offline offenders and answering the question if youth crime shifts online, the report does not distinguish between cyber-dependent and cyber-enabled offenses. In general, online offenders between 12- and 17 years old use less drugs and tend to disapprove of offline offending more. For 18–22-year-olds, online offenders use less drugs, are less often victims of offline offenses, and have fewer offline delinquent friends (Rokven et al. 2017b, 2018).

In order to examine the possible shift toward online offending, the authors used three different types of analyses. First, two types of crime (online threats and distributing viruses) had been measured in previous waves. While there is a decrease of traditional offending, these two cyber-offenses neither increase nor decrease. This does not clearly indicate any shift toward online crime, but note that these are only two types of offending that are not the most prevalent types of offending. Second, based on correlates for offending, the researchers see that exposure to risk factors for offline offenses decreases, which may reduce offline offending but does not point in the direction of a shift toward online offending. However, lastly they used predictions based on previous waves to see if juveniles who were expected to commit offline offenses actually commit online offenses. For a small proportion of the 12–17-year-olds, this points in the direction that they shifted to online crime. Rokven et al. (2017b) conclude that there is a limited evidence for a shift to online offending among youth.

Conclusion and Discussion

In this chapter, some unique samples and methodologies for studying hacking have been discussed, with a focus on Dutch research and research from other non-English-speaking countries. It showed that, in addition to the international literature, these studies provide important insights into hacking. Nevertheless, comparing the results from research in different countries based on different samples and methodologies is difficult. It is unclear if differences between countries are the result of different methodologies or country-specific differences in offenders. Therefore, future steps in a thorough understanding of hacking are international comparisons of offenders. Just as with international victimization surveys and their comparison with respect to cybercrime victimization (Levi 2017), this type of comparison may also aid our understanding of hacking.

Internationally comparing known offenders registered by the police will tell us something about the police focus or specific hard-to-find offenders, while comparisons based on general population samples tell us about more general differences in offending. Right now, existing cross-country comparisons focus on samples of college students (Chua and Holt 2016; Hu et al. 2013). Chua and Holt (2016), for example, found differences in neutralization techniques between the United States, Taiwan, and South Africa. Other studies with international samples are generally still highly focused on one or a few countries (Chiesa et al. 2008; Woo 2003), and differences between countries are not the focus of these studies. An important challenge in future research will be finding unknown hacker populations. How do we find the hackers who are not open about their hacking, not caught, and not attending hackers' conferences? The media often discusses Russian or Asian hackers, but these are less easy to study. Only a handful of research from Russian or Asian countries is published in English (Henderson 2007; Voiskounsky and Smyslova 2003) of which some are based on college students and very broad categories of cyber-offending (Hu et al. 2013; Palesh et al. 2004; Xu et al. 2013). Research on Russian language forums (sometimes together with English-language forums), however, has provided some additional knowledge on how these offender groups interact on forums (Holt 2013; Holt et al. 2012b, 2016a, b).

Interesting international comparative approaches are also macro level cross-country comparisons on, for example, law enforcement strategies against hackers (Png and Wang 2007). In that respect, preventive measures or interventions and specific laws in specific countries also provide opportunities. By looking across the border for interventions in other countries, new ideas for preventing criminal hacking may arise. Knowledge on international differences in offender characteristics may help in evaluating which interventions from other counties may be helpful. A recent international literature review has indicated that there are basically no empirically evaluated interventions for hacking that seem to have a substantial effect (Oosterwijk and Fischer 2017). However, new initiatives are starting which are partly based on the information provided in this chapter, for example, the Dutch Hack_Right intervention for highly skilled cyber-dependent first offenders (Pieters 2018; www.om.nl 2018; www.politie.nl 2018). In addition, different ways in which countries handle vulnerability disclosures (Van't Hof 2016; Van Der Wagen 2018a; Weulen Kranenbarg et al. 2018a) can provide opportunities for studying the decision-making process of both white hat and black hat hackers. In sum, studying similarities and differences between countries on both the micro and macro level can aid prevention and intervention programs against criminal hacking.

Cross-References

- ▶ Applying the Techniques of Neutralization to the Study of Cybercrime
- ▶ Computer Hacking and the Hacker Subculture
- ▶ Defining Cybercrime

- ▶ Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime
- ▶ Organized Crime and Cybercrime
- ▶ Routine Activities
- ▶ Subcultural Theories of Crime
- ▶ The General Theory of Crime

References

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

Beerthuizen, M. G. C. J., Tollenaar, N., & Van Der Laan, A. M. (2017). *The psychometric characteristics of the MZJ questionnaire on digitized, cyber and offline crime among youth. [De Psychometrische Kenmerken Van De Mzjvragenlijst over Gedigitaliseerde, Cyber- En Offlinedelicten Bij Jongeren. Schaalconstructen, Afnamemodi En Omvangschattingen.]*. Retrieved from https://www.wodc.nl/binaries/Cahier%202017-4_2699b_Volledige%20tekst_nw_tcm28-250944.pdf

Berg, M. T., & Felson, R. B. (2016). Why are offenders victimized so often? In C. A. Cuevas & C. M. Rennison (Eds.), *The Wiley handbook on the psychology of violence* (pp. 49–65). West Sussex: Wiley.

Bijlenga, N., & Kleemans, E. R. (2018). Criminals seeking ICT-expertise: An exploratory study of Dutch cases. *European Journal on Criminal Policy and Research, 24*(3), 253–268.

Bossler, A. M., & Burruss, 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* (pp. 38–67). New York: Information Science Reference.

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

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M. A., Pool, R. L. D., De Poot, C. J., Werner, Y., & Korsell, L. (2016). *Cyber-OC-scope and manifestations in selected Eu member states*. Retrieved from https://bra.se/download/18.5484e1ab15ad731149e13e0d/1490082079522/2016_Cyber-oc_-_scope_and_manifestations_in_selected_eu_member_states.pdf

Chan, D., & Wang, D. (2015). Profiling cybercrime perpetrators in China and its policy countermeasures. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 206–221). London: Palgrave Macmillan UK.

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.

Chua, Y.-T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders, 11*(4), 534–555.

De Bruijne, M., Van Eeten, M., Hernández Gañán, C., & Pieters, W. (2017). *Towards a new cyber threat actor typology a hybrid method for the NCSC cyber security assessment*. Retrieved from https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170–186). New York: Information Science Reference.

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.

Fotinger, C., & Ziegler, W. (2004). *Understanding a hacker's mind: A psychological insight into the hijacking of identities*. Retrieved from http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology, 19*(1), 112–130.

Grabosky, P. N. (2017). The Evolution of Cybercrime, 2006–2016. In T. J. Holt (Ed.), *Cybercrime Through an Interdisciplinary Lens* (pp. 15–36). New York: Routledge.

Grabosky, P. N., & Walkley, S. (2007). Computer crime and white-collar crime. In H. N. Pontell & G. L. Geis (Eds.), *International handbook of white-collar and corporate crime* (pp. 358–375). New York: Springer US.

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*, 229–243.

Henderson, S. J. (2007). *The dark visitor: Inside the world of chinese hackers*. Retrieved from http://www.lulu.com/items/volume_62/2048000/2048958/4/print/2048958.pdf

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. (2009). *The attack dynamics of political and religiously motivated hackers.* Paper presented at the Cyber Infrastructure Protection conference, New York.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165–177.

Holt, T. J., & Kilger, M. (2008). *Techcrafters and makecrafters: A comparison of two populations of hackers.* Paper presented at the WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008, WISTDCS'08, Amsterdam.

Holt, T. J., & Kilger, M. (2012). Know your enemy: The social dynamics of hacking. *The Honeynet Project.* Retrieved from https://honeynet.org/papers/socialdynamics

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. (2012a). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378–395.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012b). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891–903.

Holt, T. J., Smirnova, O., & Chua, Y.-T. (2016a). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior, 37*(4), 353–367.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016b). Examining signals of trust in criminal markets online. *Journal of Cybersecurity, 2*(2), 137–145.

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., & Chua, Y.-T. (2016). Gendering cybercrime. In T. J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 167–188). London: Routledge.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior, 37*(10), 1163–1178.

Internet Live Stats. (2018). Internet users by country (2016). Retrieved from https://www.internetlivestats.com/internet-users-by-country/

Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior, 17*(1), 16–26.

Jordan, T., & Taylor, P. A. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.

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.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018a). Criminal cashflow and it: About innovative methods, old certainties and new bottlenecks [Criminele Geldstromen En Ict: Over Innovatieve Werkwijzen, Oude Zekerheden En Nieuwe Flessenhalzen]. *Justitiële Verkenningen, 44*(5), 23–39.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018b). *Organized crime and it [Georganiseerde Criminaliteit En Ict]*. Retrieved from https://www.wodc.nl/binaries/Cahier%202018-8_2437_Volledige%20tekst_nw_tcm28-328677.pdf

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM, 52*(12), 141–144.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 225–258). Cambridge, MA: MIT Press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. New York: Oxford University Press.

Lauritsen, J. L., & Laub, J. H. (2007). Understanding the link between victimization and offending: New reflections on an old idea. In M. Hough & M. Maxfield (Eds.), *Surveying crime in the 21st century* (Vol. 22, pp. 55–75). Monsey: Criminal Justice Press.

Lee, B. H. (2018). Explaining cyber deviance among school-aged youth. *Child Indicators Research, 11*(2), 563–584.

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., De Poot, C. J., Verhoeven, M. A., Kleemans, E. R., & Lavorgna, A. (2017). Cybercriminal networks. In E. R. Leukfeldt (Ed.), *Research agenda: The human factor in cybercrime and cybersecurity* (pp. 33–44). Den Haag: Eleven International Publishing.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology, 57*(3), 704–722.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39–53.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21–37.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017d). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist, 61*(11), 1387–1402.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change, 67*(1), 3–20.

Lusthaus, J. (2018). Honour among (cyber)thieves? *European Journal of Sociology, 59*(2), 191–223.

Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, 1–11. https://doi.org/10.1093/police/pax042.

Macdonald, M., & Frank, R. (2017). The network structure of malware development, deployment and distribution. *Global Crime, 18*(1), 49–69.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(1), 191–216.

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.

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 emperical exploration of social learning theory and computer crime. *Journal of Crime and Justice, 32*(1), 1–34.

National Crime Agency. (2017). *Pathways into cyber crime*. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Computer Law & Security Review, 21*(5), 408–414.

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & De Poot, C. J. (2017). *Organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. Retrieved from https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf

Odinot, G., De Poot, C. J., & Verhoeven, M. A. (2018). The nature of and tackling organized cybercrime: Results from an international empirical study [De Aard En Aanpak Van Georganiseerde Cybercrime: Bevindingen Uit Een Internationale Empirische Studie]. *Justitiële Verkenningen, 44*(5), 9–22.

Oosterwijk, K., & Fischer, T. F. C. (2017). *Interventions young cyber offenders [Interventies Jeugdige Daders Cybercrime]*. Retrieved from https://www.wodc.nl/binaries/2779_Volledige_Tekst_tcm28-269099.pdf

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.

Pieters, J. (2018). Dutch police send young hackers to intern at it companies. *NLTimes*. Retrieved from https://nltimes.nl/2018/12/18/dutch-police-send-young-hackers-intern-companies

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.

Pontell, H., & Rosoff, S. (2009). White-collar delinquency. *Crime, Law and Social Change, 51*(1), 147–162.

Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM, 52*(4), 42–47.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a441249.pdf

Research and Documentation Center. (2018). Organized crime monitor. Retrieved from https://english.wodc.nl/Figures-and-forecasts/organized-crime-monitor/

Rogers, M. K. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf

Rokven, J. J., Tolsma, J., Ruiter, S., & Kraaykamp, G. (2016). Like two peas in a pod? Explaining friendship selection processes related to victimization and offending. *European Journal of Criminology, 13*(2), 231–256.

Rokven, J. J., de Boer, G., Tolsma, J., & Ruiter, S. (2017a). How friends' involvement in crime affects the risk of offending and victimization. *European Journal of Criminology, 14*(6), 697–719.

Rokven, J. J., Weijters, G., & Van Der Laan, A. M. (2017b). *Juvenile delinquency in the virtual world: A new type of offedenders or new opportunities for traditional offenders? [Jeugddelinquentie in De Virtuele Wereld: Een Nieuw Type Daders of Nieuwe Mogelijkheden Voor Traditionele Daders?]*. Retrieved from https://www.wodc.nl/binaries/Cahier%202017-2_2699a_Volledige%20tekst_nw2_tcm28-250948.pdf

Rokven, J. J., Weijters, G., Beerthuizen, M. G. C. J., & Van Der Laan, A. M. (2018). Juvenile delinquency in the virtual world: Similarities and differences between cyber-enabled, cyber-dependent and offline delinquents in the Netherlands. *International Journal of Cyber Criminology, 12*(1), 27–46.

Ruiter, S., & Bernaards, F. (2013). Are crackers different from other criminals? A comparison based on Dutch suspect registrations [Verschillen Crackers Van Andere Criminelen? Een Vergelijking Op Basis Van Nederlandse Verdachtenregistraties]. *Tijdschrift voor Criminologie, 55*(4), 342–359.

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.

Smith, R. G. (2015). Trajectories of cybercrime. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 13–34). London: Palgrave Macmillan UK.

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

Statistics Netherlands. (2018). *Safetymonitor 2017 [Veiligheidsmonitor 2017]*. Retrieved from http://www.veiligheidsmonitor.nl/dsresource?objectid=885

Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *British Journal of Criminology, 55*(1), 125–145.

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London: Routledge.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8–23.

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. (2009). The rhetoric of hackers' neutralizations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 317–335). Upper Saddle River: Pearson Education.

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.

Van Der Heijden, P. G. M., Cruyff, M. J. L. F., & Van Gils, G. H. C. (2017). *Methods research dark number young cyber-enabled and cyber-dependent offenders [Methodenonderzoek Dark Number Jeugdige Daders in Nederland Van Gedigitaliseerde Criminaliteit En Cybercriminaliteit]*. Retrieved from https://www.wodc.nl/binaries/2581_Volledige_Tekst_tcm28-288015.pdf

Van Der Laan, A. M., & Beerthuizen, M. G. C. J. (2018). *Monitor juvenile crime 2017: Developments in registered juvenile crime between 2000 and 2017 [Monitor Jeugdcriminaliteit 2017. Ontwikkelingen in De Geregistreerde Jeugdcriminaliteit in De Jaren 2000 Tot 2017]*. Retrieved from https://www.wodc.nl/binaries/Cahier%202018-1_2849a_Volledige%20tekst_nw_tcm28-306193.pdf

Van Der Laan, A. M., & Goudriaan, H. (2016). *Monitor juvenile crime. Developments in juvenile crime between 1997 and 2015 [Monitor Jeugdcriminaliteit. Ontwikkelingen in De Jeugdcriminaliteit 1997 Tot 2015]*. Retrieved from https://www.wodc.nl/binaries/cahier-2016-1-volledige-tekst_tcm28-74162.pdf

Van Der Wagen, W. (2018a). The cyborgian deviant: An assessment of the hacker through the lens of actor-network theory. *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 157–178.

Van Der Wagen, W. (2018b). *From cybercrime to cyborgcrime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory.* Doctoral dissertation, Rijksuniversiteit Groningen Erasmus Universiteit Rotterdam, The Netherlands. Retrieved from https://www.rug.nl/research/portal/en/publications/from-cybercrime-to-cyborg-crime(f3a5c5e0-ff0f-4dad-ac6c-2bc91d96a1b4).html

Van Der Wagen, W., & Bernaards, F. (2018). The 'non-human (f) actor' in cybercrime: Cybercriminal networks from a 'cyborg crime'-perspective [De 'non-Human (F) Actor' in Cybercrime: Cybercriminele Netwerken Beschouwd Vanuit Het 'cyborg Crime'-Perspectief]. *Justitiële Verkenningen, 44*(5), 54–67.

Van Der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *The British Journal of Criminology, 55*(3), 578–595.

Van Der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 1–18. https://doi.org/10.1177/1477370818812016.

Van Der Wagen, W., Althoff, M., & Swaaningen, R. (2016). The other 'others' [De Andere 'Anderen']. *Tijdschrift over Cultuur & Criminaliteit, 6*(1), 27–41.

Van't Hof, C. (2016). *Helpful hackers: How the Dutch do responsible disclosure*. Rotterdam: Tek Tok Uitgeverij.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-based model of computer hackers' motivation. *Cyberpsychology & Behavior, 6*(2), 171–180.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An ermpirical comparison.* Doctoral dissertation, Vrije Universiteit (VU) Amsterdam, The Netherlands. Retrieved from http://dare.ubvu.vu.nl/handle/1871/55530

Weulen Kranenbarg, M., Van Der Laan, A. M., De Poot, C. J., Verhoeven, M. A., Van Der Wagen, W., & Weijters, G. (2017). Individual cybercrime offenders. In E. R. Leukfeldt (Ed.), *Research agenda: The human factor in cybercrime and cybersecurity* (pp. 23–32). Den Haag: Eleven International Publishing.

Weulen Kranenbarg, M., Holt, T. J., & Van Der Ham, J. (2018a). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science, 7*(1), 16.

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J.-L., & Bernasco, W. (2018b). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology, 4*(3), 343–364.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior, 40*(1), 40–55.

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J. L. (2019). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology.* Advance online publication, https://doi.org/10.1177/1477370819849677

White, K. (2013). The rise of cybercrime 1970 through 2010. A tour of the conditions that gave rise to cybercrime and the crimes themselves. Retrieved from http://www.slideshare.net/bluesme/the-rise-of-cybercrime-1970s-2010-29879338

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review, 26*(3), 317–333.

Woo, H.-J. (2003). *The hacker mentality: Exploring the relationship between psychological variables and hacking activities.* Athens: The University of Georgia. Retrieved from https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf

www.om.nl. (2018). Hack_Right: Young hackers on the right path [Hack_Right: Jonge Hackers Weer Op Het Rechte Pad]. Retrieved from https://www.om.nl/@104728/hack-right-jonge/

www.politie.nl. (2018). Hack_Right: Young hackers on the right path [Hack_Right: Jonge Hackers Weer Op Het Rechte Pad]. Retrieved from https://www.politie.nl/nieuws/2018/december/18/hack-right-jonge-hackers-weer-op-het-rechte-pad.html

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64–74.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management, 24*(4), 281–287.