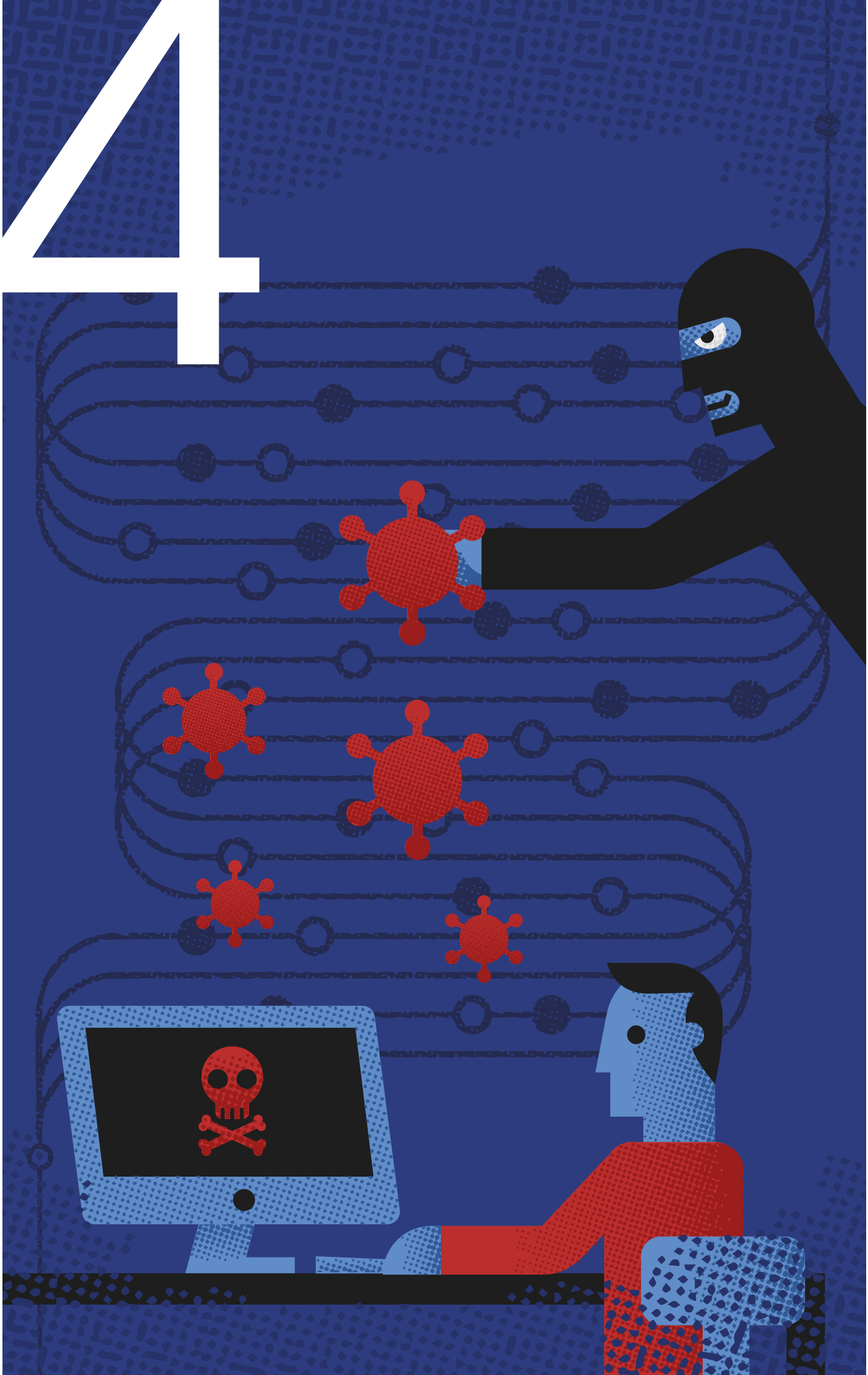
Individual cybercrime offenders

Weulen Kranenbarg, Marleen; van der Laan, André; de Poot, C.J.; Verhoeven, Maite; van der Wagen, Wytske; Weijters, Gijs

published in
Research Agenda: The Human Factor in Cybercrime and Cybersecurity
2017

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



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.