VU Research Portal

Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime

Leukfeldt, E. Rutger; Kleemans, Edward R.

published in

Researching Cybercrimes
2021

DOI (link to publisher)

[10.1007/978-3-030-74837-1_7](https://doi.org/10.1007/978-3-030-74837-1_7)

document version

Publisher's PDF, also known as Version of record

document license

Article 25fa Dutch Copyright Act

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Leukfeldt, E. R., & Kleemans, E. R. (2021). Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime. In A. Lavorgna, & T. J. Holt (Eds.), *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches* (pp. 127-144). Springer. https://doi.org/10.1007/978-3-030-74837-1_7

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

7

Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime

E. Rutger Leukfeldt and Edward R. Kleemans

Introduction

Cybercrime researchers try to understand why cybercrime occurs. Researchers have a variety of research methods at their disposal to study offenders (see, for an overview, Gadd et al., 2012). Each method has its own pros and cons and, ideally, multiple methods are used to improve our understanding of cybercrime and cybercriminals. Cybercrime researchers have used both fairly traditional methods and relatively new research methods. Traditional methods include offender interviews, surveys, and ethnographic research (see, for instance, Holt, 2009;

E. R. Leukfeldt (✉)

Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)
and The Hague University of Applied Sciences, Amsterdam, The Netherlands
e-mail: RLeukfeldt@nscr.nl

E. R. Kleemans

Vrije Universiteit Amsterdam, Amsterdam, The Netherlands
e-mail: e.r.kleemans@vu.nl

Weulen Kranenbarg, 2018), as covered more in details in Chapters 6, 14, and 24–26 of this book. The innovative methods used by cybercrime researchers are often linked to the unique opportunities the internet creates to gather data about criminals who use the very same internet to commit their crimes. Examples include scraping data from criminal forums and markets on both the clear web and the dark web (Dupont et al., 2017; Hutchings & Holt, 2015; see Chapters 10, 11, 13, and 22), using publicly available online data (see also Chapters 8 and 9), and using honey pots to study attacker behavior (see Chapter 12).

Currently, cybercrime research is still in its infancy. Although an increasing number scholars from various disciplines are involved in cybercrime studies, many of the “big” questions remain unanswered (see, e.g., Holt and Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019). A major problem is that it is simply difficult to study the criminals committing cybercrimes. Indeed, criminals try to hide their illegal activities and are usually not disposed to talking openly to researchers, which limits the usefulness of the more traditional social sciences’ research methods. Furthermore, the innovative methods come with their own limitations: Although they usually provide big datasets with sometimes hundreds of thousands of data points, they only provide superficial data or, in the case of scraped data, only contain information about one very small step in the crime scripts of cybercriminals. In-depth police investigations, therefore, can be very useful as an extra tool in the toolbox of cybercrime researchers. Indeed, these investigations provide a unique insight into cybercriminal networks and their members because of the wide use of intrusive investigation methods, such as wiretaps, IP taps, observations, undercover policing, and house searches. Together with more traditional methods (such as interviews and surveys) and innovative methods (such as analysis of scraped data or open source data), police files can be used to improve our understanding of cybercrime and offender behavior.

Getting access to police data can be difficult. Hence, scientific progress in cybercrime research is hindered by the general lack of cooperation between the police and academic researchers. For outside academic observers, only the tip of the iceberg of cybercrime is visible and much of the iceberg is only revealed if the police use special investigative

powers such as undercover operations, wiretapping, intercepting internet communication, bugging, seizing and decrypting information on servers, house and computer searches, and interrogations. A prime example of this problem is that academic researchers are able to scrape data on the internet on a massive scale but this only provides rather superficial information about Darknet markets, since we remain unaware of structures and actions hidden behind transactions and fake identities. This underlying information only becomes available if the police target the marketplaces and academic researchers gain access to the data. Other cybercrime phenomena share similar problems for academic researchers: The incidents can be described but it often remains unclear which (cooperating) offenders and actions create the patterns that are observed. The offender perspective is often lacking and research projects to liaise with relevant cybercrime offenders are scarce. Furthermore, the efforts to persuade them to share concrete information about offender behavior and incidents have a very high cost–benefit-ratio. Lastly, this scarce information is dwarfed by the rich information that is collected by police in specific cybercrime operations. Of course, it is precisely the job of the police to break these walls of silence, but the rich information gathered in such operations often remains hidden behind other walls of silence and is not put to use for academic research. For academic research, therefore, strengthening cooperation with the police is an important endeavor that would greatly benefit theoretical and empirical progress in cybercrime research.

This chapter describes the pros and cons of using police investigations to shed light on cybercrimes. First, we describe the Dutch Organized Crime Monitor, an instrument that has been used to systematically analyze police files about organized crime (including cybercrime) for over two decades. Next, we focus on the use of police data to analyze cybercrimes. Since researchers in many countries do not have easy access to police investigations, we also discuss an alternative option: reconstructing cases based on interviewing case officers involved in criminal investigations. Lastly, based on recent publications, the chapter demonstrates how the analysis of criminal investigations can produce cybercrime knowledge which other research methods simply cannot provide: By breaking the walls of silence, police files provide a rich picture of the hidden world of cybercriminals.

The Dutch Organized Crime Monitor and Cybercrime

In the Netherlands, law enforcement institutions, such as the police and the Public Prosecution Office, are generally more willing than in other countries to cooperate in academic research, particularly in the area of organized crime and cybercrime research. This cooperative spirit may be ascribed to a rather progressive police force but also to the backlash of a huge political scandal which forcefully shattered the walls of silence of the police monopoly on information about organized crime. This scandal, the so-called IRT-affair, took place in 1994–1996 and concerned police undercover operations in organized crime, resulting in a Parliamentary Inquiry Committee into Criminal Investigation Methods. The Committee discredited existing police reports on organized crime and opened up the police for independent academic research. An external academic research group—the research group *Fijnaut*—was appointed and produced an extensive report on organized crime which was published as an appendix to the report of the committee in 1996 (Fijnaut et al., 1996, 1998; PEO, 1996). After the publication of this report, the Dutch Minister of Justice promised the Dutch Parliament to produce reports on a regular basis on the nature of organized crime in the Netherlands. From 1996 onwards, the Dutch Organized Crime Monitor, a collaboration of the Research and Documentation Centre (WODC), Vrije Universiteit Amsterdam, and Erasmus University Rotterdam, has conducted an ongoing systematic analysis of closed police investigations of criminal groups to provide insight into the nature of organized crime in the Netherlands (see for a more extensive discussion of the origins and methodology of the Dutch Organized Crime Monitor, see Kleemans, 2014).

The basic idea behind the Dutch Organized Crime Monitor is to collect solid empirical data on a wide cross section of organized crime cases in order to inform policy and practice. The main sources for the Dutch Organized Crime Monitor are the closed police files of criminal groups, often spanning a period of several years (for more information, see Kleemans, 2007, 2014). In five data sweeps, 180 large-scale investigations were systematically analyzed. Major reports to Parliament were

published in 1998, 2002, 2007, 2012, 2018, and 2019 (Kleemans et al., 1998, 2002; Kruisbergen et al., 2012, 2019; Van de Bunt & Kleemans, 2007). A specific report was drafted on the topic of organized crime and IT (Kruisbergen et al., 2018) and the last data sweep also included cybercrime cases. Until the last data sweep, there were very few available large-scale investigations into cybercrime that would qualify as organized crime (see below).

Each case analysis started with structured interviews with police officers and/or public prosecutors. After these interviews, the police files (to which researchers had direct access) were analyzed and summarized, using an extensive checklist on the following topics: the police investigation and the investigation process; the criminal network; the criminal activities and modus operandi; contacts with the licit and illicit environment; criminal proceeds, investments, spending, money laundering, and seized assets; judicial procedure and verdict; and evaluation (lessons learned, new insights, prevention opportunities, new developments, effectiveness of policing strategies see Kruisbergen et al., 2019). The checklist was also used and adapted in specific research into cybercriminal networks by Leukfeldt and colleagues (e.g., Leukfeldt, 2016; Leukfeldt et al., 2017a).

Police Data and Cybercrime Research

When the Dutch Organized Crime Monitor was developed, several trade-offs had to be made. Below, we briefly review three topics and answer the question whether such trade-offs may also be germane to (certain types of) cybercrime.

Opting for Solid and “Older” Evidence

How solid should evidence be to be used in criminological research and who decides upon what amounts to being solid evidence? Tappan (1947) and Sutherland (1945) already fiercely debated this topic decades ago, as Tappan claimed that only the courts could rule whether someone

was guilty or not. Conversely, Sutherland argued that criminal activities should be investigated as close to the sources as possible; otherwise, some criminal activities, such as white-collar crime, would remain largely unexplored as a subject of criminological research.

Two aspects are relevant in this mature but still topical debate. First, the process of investigation and prosecution also involves a selection process which is influenced by police priorities, successes, and failures in criminal investigations, and all kinds of decisions and trade-offs that are made during investigation and prosecution. Second, the last part of the judicial process provides a high level of solidity (confirmed by the court, in appeal, or even by the Supreme Court) regarding an extremely small part of—very old—cases. In reality, a criminal investigation may take two to five years (or even longer), whereas waiting for a final judgment may take another five to ten years. Furthermore, judicial considerations do not always regard the solidity of evidence but may also observe formal procedures in investigation (e.g., international exchange of information) and prosecution. Consequently, exclusion of evidence on the basis of admissibility by the court does not always mean that this information is unsuitable for scientific research.

The Dutch Organized Crime Monitor opts for solid and “older” evidence and focuses on recently closed police investigations into criminal groups that provide enough evidence for the public prosecutor to take the case to court. In brief, these are “strong cases” (according to the public prosecutor) but the analysis should not wait until a final verdict has been reached. The evidence is analyzed at an earlier point in time, as soon as the first independent check (by the public prosecutor) is completed. An advantage of this timing is that the police team has just finished the largest part of the investigation and can answer a lot of the questions. In follow-up research, court cases and the procedures allowing confiscation of assets can be followed and case descriptions accordingly extended and updated.

Extensive Analysis of Rich Information

The focus on “older” cases and the extensive analysis of rich information of a large-scale police investigation, however, also have drawbacks. Case descriptions may be solid yet not very “fresh” at the time of publication. Furthermore, soft intelligence revealing new phenomena and trends might be disregarded. For this reason, during the first data sweep of the Dutch Organized Crime Monitor (1996–1998) a lot of time and effort was spent collecting all the available intelligence and crime analysis reports on organized crime in the Netherlands and many interviews were conducted with key informers in criminal intelligence units. With the benefit of hindsight, it was concluded that the cost–benefit-ratio of all these efforts was possibly too high for an empirical research project.

For cybercrime, one might argue that despite rapidly developing malware technology and criminals constantly looking for new weaknesses in the security of systems, the general business models for crimes (such as phishing, ransomware, and other cybercrimes) are quite stable and changes in crime scripts may not actually be substantial. On the other hand, one cannot know that in advance and other types of research, based on case debriefs or interviews with investigators, might also be a feasible option to include information of more recent cases. These methods might be less solid and less extensive but they may also be less labor-intensive and an appropriate alternative for more recent cybercrime cases.

Criminal Groups as Prime Target of Police Operations

The quest of the Dutch Organized Crime Monitor team to find “large-scale” cybercrime cases fitting the definition of organized crime also revealed three important insights for cybercrime research. First, many cybercrime cases do not qualify as large consolidated cases of organized crime but often concern small cases or clusters of small cases (including small cases with large impact value). Second, the criminal group is not always the prime target of police operations; instead, police operations may target markets (with neither capacity nor priority to investigate all

buyers and all vendors, all over the world); seize and decrypt information on servers; or just focus on prevention by finding the source of an incident (a hack, a virus, a DDoS-attack) and taking preventive action (e.g., by warning responsible parties and suggesting changes in software, systems, or procedures). Third, much more data can be seized during police operations into cybercrime than can be investigated by the police, given their limited capacity. Therefore, the population of cybercrime cases and cybercrime operations is rather diverse and only specific police operations can focus on a larger group of collaborating offenders carrying out activities with significant harm to society. For the last category, the extensive analysis on the Dutch Organized Crime Monitor might be the best option. For other investigations and operations, however, other types of analysis might be more appropriate and the “big data” that are seized may offer other opportunities for researchers as well.

An Alternative for Police Data: Reconstructing Case Files Based on Interviews

Reconstructing case files based on structured interviews was used as a method by Leukfeldt and colleagues in countries other than the Netherlands, where direct access to the original police files was not possible (Leukfeldt, 2016; Leukfeldt et al., 2017b). There may be several reasons why reconstructing case files based on interviews might be a good alternative for analyzing the original police data.

First, interviews provide insight into more recent cases. Police are often more willing to be interviewed on a recent case than to share all original data and all details, as the investigation may still be evolving and/or other procedures may hinder sharing data at that point in time. The interconnectedness of cases also has to be taken into account: Prosecuted cases are sometimes linked to other cases still under investigation and/or potential cases for new investigations, which gives rise to different opinions about the sensitivity of sharing information with researchers.

Second, cybercrime cases often have an international component, which means that not all data can easily be shared with researchers. For example, national investigations have spin-offs abroad in investigations

on offenders operating or residing in other countries, or data have been seized from servers abroad and have been shared with national authorities. Sharing “national” information is sometimes already difficult but the international component may add more complexity, sensitivity, and caution about sharing the original data. Sharing more abstract information about a case in a structured interview, however, may be far less sensitive and thus a viable alternative option.

Third, specific offender information is often very sensitive, particularly for offenders who are not already subjected to actual investigation and prosecution. By contrast, interviews can already shed light on phenomena and criminal activities, without sharing specific information on offenders.

Fourth, cybercrime cases sometimes result in information overflow, for instance, when communication data have been seized on servers and decrypted or when the police are able to infiltrate criminal marketplaces on the dark web. Police capacity is limited and the police simply cannot and do not want to investigate all offenders and all criminal activities, all over the world. A structured interview can be a viable alternative in such cases. Furthermore, such interviews can also be combined with a more focused analysis of specific parts of the underlying information, for instance, on interactions between the organizers of the Darknet markets (instead of all buyers, sellers, and transactions on these markets).

Proof of the Pudding: Examples of Added Value of Cybercrime Studies Based on Police Investigations

This section, based on recent publications, shows how analyzing criminal investigations can produce cybercrime knowledge other research methods simply cannot provide: by breaking the walls of silence to get a rich picture of the hidden world of cybercriminals.

One Case Can Change the Landscape

One of the first articles about cybercriminal networks based on police files was the study of Leukfeldt (2014) on phishing. The author provided an in-depth description of the *modus operandi* and organizational structure of one network active in phishing. The article demonstrated that the literature about these types of networks prior to 2014 provides an incomplete picture of the landscape of such networks. In contrast to prior research, the study showed a well-organized group of criminals whose relationships are long-lasting and based on real-world social ties rather than ad-hoc relationships formed on online meeting places, and who mainly use social engineering rather than malware as a tool to acquire information from their victims. This analysis not only had implications for the way we have to view cooperating cybercriminals, it also offered an entire set of new possibilities for situational crime prevention: The focus can be much more on real-world social ties, subcultures, and establishing trust, in addition to the technological measures which are usually aimed at disturbing online meeting places. In later studies, the importance of social ties within cybercriminal networks shown by this singular case described in Leukfeldt (2014) has been corroborated (e.g., Kruisbergen et al., 2019; Leukfeldt et al., 2017a; Lusthaus, 2018; Lusthaus & Varese, 2017).

Changing the Concept of "Organized" in Organized Crime

Bulanova-Hristova and colleagues (2016) studied police investigations in Sweden, Germany, and the Netherlands to examine the intertwinement of organized crime and cybercrime. The researchers focused on the *modus operandi*, the organizational structures of the criminal groups, and the profiles of the offenders involved in these groups. First, the authors show that the Internet enables new types of organizational structures that do not necessary fall within the traditional definitions of

organized crime. As traditional crime and cybercrime become increasingly intertwined (Kruisbergen et al., 2018; Leukfeldt, Lavorgna et al., 2017; Leukfeldt et al. 2019; Leukfeldt & Roks, 2020), this could mean a shift in the way we view organized crime groups. Furthermore, a remarkable finding of the study by Bulanova-Hristova and colleagues (2016) is that a “new type” of offender became visible in these cases: very young offenders; offenders with an IT background; and ill or disabled offenders who barely came out of their homes. In a subreport, Odinot and colleagues (2016) concluded that characteristics of offenders which are important in the offline world, such as age, physical health, and social behavior, seem to be less important for organized cybercrime.

Mapping Hidden Social Processes

Police files can be used to gain insight into social processes within cybercriminal networks. These processes have always been very important for the origin and growth of criminal networks (see, for instance, Ianni & Reuss-Ianni, 1972; Kleemans & De Poot, 2008; Bouchard & Morselli, 2014). However, increasingly, studies based on data scraped from online forums have suggested that the importance of social relations is diminishing (Décary-Héту & Dupont, 2012; Décary-Héту et al., 2012; Yip et al., 2012; Holt & Smirnova, 2014) as trust can be gained faster by using rating and review systems and geographical limitations of social networks no longer exist. However, an important limitation is that the studies based on scraped data provide an incomplete picture of criminals or networks of criminals who actually use such forums.

Using police data, Leukfeldt and colleagues (2017a) zoomed in on the importance of these online forums and markets for cybercriminal networks: Important questions were how cybercriminals meet, how cybercriminal networks develop, and what this means for the criminal capabilities of these networks. It turned out that—although online meeting places certainly did play an important role in a number of networks, for example, to find suitable co-offenders or to get into contact with enablers with highly specific knowledge or skills—traditional offline social ties still played an important role in the processes of origin and

growth of the majority of networks. Leukfeldt and colleagues (2017c) demonstrated in another article that from a crime script perspective, these forums even have a very modest role. When looking at the hidden social processes behind cybercriminal networks, cybercriminals turned out to me much more traditional than expected.

In another study, Leukfeldt and Holt (2019) examined the organizational structure of cybercriminals involved in financially motivated attacks. Although the common view of hackers is that they work alone, criminological research has shown that in general, most criminals in fact need others—with specific knowledge, contacts, or cash—to carry out their crimes (such as Andresen & Felson, 2010; Reiss & Farrington, 1991; Shaw & McKay, 1931; Sutherland, 1937). Police files provide a wealth of data about ties between criminals. Leukfeldt and Holt (2019) demonstrated, using the Best and Luckenbill (1994) sociological framework, that the majority of the networks they studied showed organizational sophistication based on their division of labor and extended duration over time. Indeed, most networks could be classified as “teams” or “formal organizations.” In contrast to prior studies—based on either interviews with individual offenders or analysis of scraped data from online meeting places—no loners were present and only a few networks could be classified as “colleagues” or “peers.” Consequently, prior studies provided an incomplete picture of criminal collaboration.

Using Interrogations to Focus on Subcultures

Police investigations usually contain the results of the use of various (special) investigative powers. Leukfeldt and Kleemans (2019) demonstrated that it is possible to use the results of police interrogations to gain unique insight into the subculture of money mules. Leukfeldt and Kleemans used fourteen Dutch criminal investigations containing interrogations of 211 money mules. As 69 suspects did not cooperate during the interrogation (“no comment”) and 30 claimed to be innocent, interrogations of 112 money mules were used in the analysis. The statements of the money mules clearly showed that they were part of a subculture where it is considered normal to be asked to cooperate in fraudulent

transactions on a daily basis (see Box 1). The analysis of these 112 interrogations can also be used to draft various situational crime prevention measures (see Leukfeldt & Kleemans, 2019).

Box 1: Subculture (Quotes from: Leukfeldt & Kleemans, 2019)

During an interrogation Suspect 38 states: “I get text messages on a regular basis from several guys. These guys ask me if I know anyone who wants to make money. They simply ask you if you have cash cards”. Suspect 38 shows a text message that she got that morning from F: “Don’t you know a girl who wants booty?”

“Since about 2 years rumor has it that you can earn easy money by providing your bank account. Also through the Internet messages are sent that you can earn money by offering your bank account. I didn’t want to cooperate, I am not a money mule or errand-boy. Some months ago I changed my mind. I really could use the money. I ran into a Surinamese boy and he introduced me to S1”.

Suspect 9 states: “This is general knowledge in Amsterdam. It’s a big hit. They do it with everything. They earn a lot of money with fraud”. About the person to whom she would have offered her cash card, she states: “They call him Prince. It’s from the streets. Really, everybody knows him. He’s from Ghana. Together with his uncle he commits fraud [...], I said already that everybody in the Netherlands is involved. Many people do it. Especially youngsters. You can earn easy money and many want to do that. Many youngsters or junkies who have nothing to lose”.

Conclusion

Cybercrime is on the rise, and with the ongoing digitization of our society, it will probably keep rising in the near future. Insight into cybercrime and offender behavior, therefore, is necessary to develop measures to prevent criminals from successfully carrying out attacks. In this chapter, we demonstrated the added value of analyzing police investigations—or alternatively case reconstructions based on interviews—to

improve our understanding of cybercriminals. We do not claim that only police files should be used to study cybercriminals. Both traditional and innovative research methods should be used to collect as much information as possible, ideally within the same study (ensuring triangulation). However, we would like to emphasize that analyzing police files yields unique and rich information about important processes within criminal networks that often remain hidden when using other research methods. Without the studies based on police files, we would not have had so much detailed information about the processes of origin and growth of cybercriminals networks; the hidden subcultures; and the intertwinement of traditional crime and cybercrime.

We acknowledge that in some countries it is difficult or even impossible to get access to police files. However, the examples in this chapter of cybercrime studies based on police investigations clearly show that in many countries this is a feasible option: researchers in the Netherlands, Germany, and Sweden got access to police files and, in countries such as the UK and the USA, case reconstructions based on interviews with case officers were carried out. Indeed, it might be hard to get access but not impossible, and once researchers get such access, this is extremely useful in breaking down the walls of silence.

References

- Andresen, M. A., & Felson, M. (2010). Situational crime prevention and co-offending. *Crime Patterns and Analysis*, 3(1), 3–13.
- Best, J., & Luckenbill, D. F. (1994). *Organizing deviance* (2nd ed.). Prentice Hall.
- Bouchard, M., & Morselli, C. (2014). Opportunistic structures of organized crime. In L. Paoli (Ed.), *The Oxford handbook of organized crime*. Oxford University Press.
- Bulanova-Hristova, G., Kasper, K., Odinet, G., Verhoeven, M., Pool, R., de Poot, C., Werner, W., & Korsell, L. (Eds.). (2016). *Cyber-OC—Scope and manifestations in selected EU member states*. Bundeskriminalamt.
- Décary-Héту, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, 13(3), 160–175.

- 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.
- Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of “the most dangerous cybercrime forum in the world.” *American Behavioral Scientist*, 61(11), 1219–1243.
- Fijnaut, C., Bovenkerk, F., Bruinsma, G., & van de Bunt, H. (1996). Bijlage VII: Eindrapport Onderzoeksgroep Fijnaut. In Parlementaire Enquêtecommissie Opsporingsmethoden (PEO), *Inzake opsporing: Enquête opsporingsmethoden*. Sdu Uitgevers.
- Fijnaut, C., Bovenkerk, F., Bruinsma, G., & van de Bunt, H. (1998). *Organized crime in the Netherlands*. Kluwer Law International.
- Gadd, D., Karstedt, S., & Messner, S. F. (Eds.). (2012). *The SAGE handbook of criminological research methods*. <https://doi.org/10.4135/9781446268285>.
- Holt, T. J. (2009). Lone hacks or group cracks: Examining the social organization of computer hackers. *Crimes of the Internet*, 336–355.
- 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., & Smirnova, O. (2014). *Examining the structure, organization, and processes of the international market for stolen data*. U.S. Department of Justice.
- Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3), 596–614.
- Ianni, F. A. J., & Reuss-Ianni, E. (1972). *A family business: Kinship and social control in organized crime*. Routledge and Kegan Paul.
- Kleemans, E. R. (2007). Organized crime, transit crime, and racketeering. In M. Tonry & C. J. Bijleveld (Eds.), *Crime and justice: A review of research* 35. The University of Chicago Press.
- Kleemans, E. R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson & E. Cockbain (Eds.), *Applied police research: Challenges and opportunities*. Crime Science Series. Willan.
- Kleemans, E. R., Brienen, M. E. I., & Van de Bunt, H. G. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. WODC.
- 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.

- Kleemans, E. R., van den Berg, E. I. A. M., & Van de Bunt, H. G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. WODC.
- Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. (2018). *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. WODC.
- Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. (2019a). Money talks: Money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, 42(5), 569–581.
- Kruisbergen, E. W., Roks, R. A., & Kleemans, E. R. (2019b). *Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. Boom.
- Kruisbergen, E. W., van de Bunt, H. G., & Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Boom.
- Leukfeldt, E. R. (2014). 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. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International Publishing.
- Leukfeldt, E. R. (Ed.). (2017). *Research agenda: The human factor in cybercrime and cybersecurity*. Eleven International Publishers.
- Leukfeldt, E. R., & Holt, T. J. (2019). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology*, 64(5), 522–538.
- Leukfeldt, E. R., & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention. In S. Hufnagel & A. Moiseienko (Eds.), *Criminal networks and law enforcement: Global perspectives on illicit enterprise*. Routledge.
- 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. *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, 39–53.

- Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, 61(11), 1387–1402.
- Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287–300.
- Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. (2019). Criminal networks in a digitized world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-019-09366-7>.
- Leukfeldt, E. R., & Roks, R. (2020). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior* (online first).
- Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.
- Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice* (online first).
- Maimon, D., & Louderback, E. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2, 191–216.
- 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*. WODC.
- PEO. (1996). Parlementaire Enquêtecommissie Opsporingsmethoden. In *Inzake opsporing: Enquête opsporingsmethoden*. Sdu Uitgevers.
- Reiss, A. J., & Farrington, D. P. (1991). Advancing knowledge about co-offending: Results from a prospective longitudinal survey of London males. *Journal of Criminal Law and Criminology*, 82(2), 360–395.
- Shaw, C. R., & McKay, H. D. (1931). *Report on the causes of crime: Volume II*. Government Printing Office.
- Sutherland, E. H. (1937). *The professional thief*. The University of Chicago Press.
- Sutherland, E. H. (1945). Is “white collar crime” crime? *American Sociological Review*, 10, 132–139.
- Tappan, P. (1947). Who is the criminal? *American Sociological Review*, 12, 96–102.
- Van de Bunt, H. G., & Kleemans, E. R. (2007). *Georganiseerde criminaliteit in Nederland. Derde rapportage op basis van de Monitor Georganiseerde*

Criminaliteit. Reeks Onderzoek en Beleid 252. WODC/Boom Juridische Uitgevers.

Weulen, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison*. VU University.

Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. In *IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 60–65).