Fieldwork Experiences Researching Cybercriminals

Asier Moneva (https://orcid.org/0000-0002-2156-0213)

Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) & Center of Expertise Cyber Security of The Hague University of Applied Sciences

Email: amoneva@nscr.nl (corresponding author)

Rutger Leukfeldt (https://orcid.org/0000-0002-3051-0859)

Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) & Center of Expertise Cyber Security at The Hague University of Applied Sciences

Email: rleukfeldt@nscr.nl

Marco Romagna (https://orcid.org/0000-0001-5634-7693)

Center of Expertise Cyber Security at The Hague University of Applied Sciences

Email: m.romagna@hhs.nl

This is an Author Accepted Manuscript version of the following chapter: Moneva, A., Leukfeldt, R., & Romagna, M. Fieldwork Experiences Researching Cybercriminals, published in Fieldwork Experiences in Criminology and Security: Methods, Ethics, and Emotions, edited by A. Diaz, C. Del-Real, and L. Molnar (in press), Springer Nature.

Chapter.
Fieldwork Experiences Researching Cybercriminals

Abstract: Cybercriminals are an elusive population to study. This makes social research with cybercriminals as valuable as it is scarce. To stimulate research on cybercriminals, it is important that researchers share their insights on successful and unsuccessful approaches, strategies, and techniques. This chapter collects our fieldwork experiences researching cybercriminals, potential cybercriminals, hackers, and hacktivists. After presenting the phases of our fieldwork, we outline six research techniques we have applied and discuss the ethical issues involved. We conclude with some lessons learned and methodological perspectives to guide future research.

1.1 Introduction

To better understand cybercrime and improve cybersecurity in highly digitalized societies, it is increasingly important to broaden knowledge about actors capable of exploiting information technologies: we refer to cybercriminals. Researching cybercriminals, however, can often be challenging as they tend to operate 'in the dark' and stay under the radar.

This chapter is about our field experiences researching cybercriminals. Our experiences include direct contact through interviews, administration of questionnaires, and participation in capture-the-flag exercises; and indirect contact through analysis of self-reported data, and analysis of large-scale police investigations. Note that, although in many cases we focus on specific cybercriminals such as criminal hackers, the insights we gained from our research—which we show here—can also be applied to cybercriminals more generally. This is one of the things you first learn when you do fieldwork: no two cybercriminals are alike. The organized phisher who targets elderly people has little to do with the loner hacktivist who protests on social media; the experienced hacker who encrypts organizational data for ransom is quite different from the script kiddie who defaces a website to gain status. Moreover, categories are often blurred as actors can play different roles at the same time. What are then hackers? How do they identify themselves? Are they different from cybercriminals? Cybercriminals often combine different cybercrimes with traditional deception techniques. Some do hacking, but also phishing, and offline social engineering.

1.2 Cybercrime and hacking, cybercriminals and hackers

Lay people often think that cybercrime is highly technical. The truth is that sometimes it is, but many times it is not. There are different degrees of technification. Cyber-dependent crimes would be those more technical crimes that did not exist before the Internet, and that use computers to attack other computers, like hacking, malware infection, or denial of service (DoS) attacks; cyber-enabled crimes—in contrast—would be those not so technical crimes that already existed before the Internet did, and that usually target people, like fraud, stalking or

sexual harassment (McGuire, 2020; McGuire and Dowling, 2013). Annual Internet crime reports from the FBI suggest that cyber-enabled crimes are far more prevalent than cyber-dependent crimes, especially phishing and its variants. In 2021, 323,972 victims of phishing, vishing, smishing, and pharming attest that social engineering—a not necessarily technological strategy—is frequently used by cybercriminals to reap about $44,213,707 in profits (Internet Crime Complaint Center, 2021).

Like cybercrime, hacking varies technically. Legal definitions of hacking refer to entering computer systems without permission (i.e., trespassing). In this sense, a hack can consist of a backdoor virus attack, a SQL injection, a brute force attack, a phishing attack, or copying a user's password from a post-it. It can therefore range from techniques that require advanced programming knowledge to techniques that do not require any IT knowledge at all. Extralegal definitions are much broader and focus on behavioral aspects around the application of IT knowledge (Holt, 2020; Yar and Steinmetz, 2019). For example, Steinmetz defines hacking as "a transgressive craft".

Within the category 'cybercriminals' there are also notable differences. In cybercrime studies, the hacker is often considered a sub-category of cybercriminal, but the concepts of cybercriminal and hacker are in fact fluid; they can just as easily be (erroneously) interchanged as not at all (Yar and Steinmetz, 2019). Originally the term hacker had a positive connotation—or at least not a negative one. Malicious actors were in fact known as *crackers*. Later on this distinction faded away, although many members of the hacking community still object when both groups are conflated (Jordan, 2017). To make matters worse, there are also different types of hackers. For example, malicious or *black-hat* hackers look for vulnerabilities in computer systems with criminal intent, while ethical or *white-hat* hackers look for vulnerabilities to reinforce cybersecurity. When hackers are initiating their criminal career, they are called script-kiddies, usually young novices who seek to gain status in the hacker community with their illicit activities (Holt, 2007). And if they have a socio-political agenda, hackers are often called hacktivists (Romagna, 2020). Others simply hate labels. In any case, it is rare that criminal hackers only do hacking. More often they perform a range of malicious activities such as writing malware to encrypt data, or infecting botnets to carry out DDoS attacks, either individually or as part of a criminal organization. Within criminal organizations, hackers can have different roles: from executors of technical tasks to enablers for those who do not have sufficient technical knowledge (e.g. Leukfeldt and Holt, 2022). This is why researching hackers often overlaps with researching cybercriminals.

1.3 Phases of fieldwork

Over the last decades, criminologists have had to adapt to new forms of crime, offenders with unique characteristics, and online environments where crime occurs, hence developing new methodologies for online fieldwork (Holt and Bossler, 2016; Lavorgna and Holt, 2021). Based on our experience, here we explain a series of standard fieldwork phases for researching cybercriminals that range from initial reconnaissance to contact with the subjects.

1.3.1 Understand the hacker subculture

Hackers are not like other cybercriminals. Think of the average scammer, for example; they will generally share neither motivations, nor skills, and possibly not even sociodemographic background with hackers. Many hackers do not even consider themselves offenders (e.g. Holt, 2007), and they have their own ethics (Levy, 1984). Their belief system articulates around technology, knowledge, and secrecy (for a review see Holt, 2020). It was not until the late 20th century that hackers began to be portrayed as criminals (Taylor, 1999).

The first challenge for the researcher is therefore to define what hacking is. Currently, the illegality of their actions is determined in many legislations by whether or not they have permission to trespass a system (Wall, 2001; Yar and Steinmetz, 2019). This puts even white-hat hackers in a difficult position that may deter them from carrying out cybersecurity exercises, such as bug bounties (Del-Real and Rodriguez Mesa, 2022). It is therefore a thin line that separates black from white which often situates hacking in a gray area. Other works adopt broader definitions beyond mere legal considerations (e.g. Schell and Dodge, 2002; Steinmetz, 2015). Researchers must keep this in mind when dealing with hackers and also when interpreting their research data.

1.3.2 Take care of legal and cybersecurity issues

Before contacting cybercriminals or others associated with them, it is important to adopt minimum privacy and cybersecurity protection measures. The coverage of these measures must be in accordance with the research design and reach all actors involved: researchers, subjects, third parties (e.g. police, consultancy), and their institutions. It must be also be noted that an aggressive reaction from a single hacker in response to the researcher's approach can cause significant disruption. It is therefore advisable to consider at least two aspects when contacting cybercriminals to collect and store data securely: complying with legal requirements and using appropriate infrastructure and materials.

Researchers can prepare legal documents to agree in advance on elements such as the explicit consent of the subjects to participate in the research; the non-disclosure of sensitive information; the form and limits of the collaboration between the parties; and the type of data that will be collected and shared: where, how and until when they will be stored, who will have access to them, and the conditions under which, if applicable, they will be published. In Europe, the General Data Protection Regulation (GDPR) regulates the processing and movement, as well as the protection, of data of individuals (European Parliament and Council of the European Union, 2016). Some institutions have Data Protection Officers who can guide the researcher throughout this whole process.

Many research designs rely on infrastructure to collect data. For example, interviews may require a private space and hardware such as an ecrypted voice recorder. Other studies may require the use of infrastructure such as computer labs with specific software to collect data (e.g. video, keylogger), antivirus software to protect the institution, or VPN to add a layer of anonymization. Note that the use of VPN can be a double-edged sword: although it can be

a means of protection, participants might get suspicious with it. In fact a VPN can be seen as a tool used by law enforcement agencies to mask their real location and would therefore trigger a red flag, immediately undermining the relationship between interviewer and interviewee to the point of keeping away possible respondents.

1.3.3 Find the population of study

It is precisely the secrecy mentioned above that makes it difficult to contact cybercriminals for research, let alone hackers. Difficult is not impossible though. There are online environments—such as forums, chats, and social media—where cybercriminals socialize with their peers and share knowledge (Leukfeldt et al., 2017a, 2017b). A few examples are Hack Forums, Reddit, and Telegram. Not all cyber places are equally public (Miró-Llinares and Johnson, 2018; Moneva, 2020), and it is probably in the most private places where the most experienced cybercriminals are to be found and where communication is most free. Sometimes it is also possible to contact offenders who are in contact with the criminal justice system because they are serving a rehabilitative sentence; for example, through probation services or participation in educational programs (Schiks et al., 2021). The problem with this strategy is that samples tend to over-represent novice hackers or script-kiddies, and under-represent more experienced cybercriminals who have not been identified or arrested.

When researchers are unable to recruit actual cybercriminals they often resort to convenience samples with similar sociodemographic characteristics and expertise, usually represented by IT experts or students (e.g. Holt et al., 2012; Marcum et al., 2014). Although some researchers question the external validity of the results obtained with such samples, others argue that they are adequate for studying topics like cybercrime involvement (see Chua and Holt, 2016).

1.3.4 Engage with cybercriminals

Different cybercriminals require different ways to establish contact. When reaching out for hackers, the best way is to look for them either in hacking forums or on social media. The next step is to establish rapport. This process can take a long time because cybercriminals are wary of new users and introducing oneself as a researcher is not helpful either. Having a public profile linked to several sources can make it easier for cybercriminals to verify your identity and not consider you a threat. Talking about common interests, news, and trivial facts can also help. Signs that rapport has been established are, for example, when respondents start making jokes and referring to your private life. Once a solid relationship is established hackers are then more likely to refer the researcher to other hackers, thus enabling a snowball sampling process. The main issue with hackers is that they are extremely suspicious and might not be interested in answering questions, particularly if researchers do not have a basic knowledge of the topics to address (Hutchings and Holt, 2018). Others, like hacktivists, tend to like visibility and are therefore more open to talk. They are easy to contact on social media such as Twitter, Facebook, and Telegram, especially if the researchers already have an active account. We have contacted 120 potential hacktivists through social media. In some cases, we used the email

addresses left on defaced websites. Of these, 50 replied, and 34 agreed to participate in interviews, for a response rate of 28.3%. Note that the platforms through which we contacted them were not necessarily the same ones through which we conducted the interviews, the latter being generally more private channels such as Telegram, Signal, and Wire (Romagna and Leukfeldt, in press) Transparency is another important matter when contacting hackers, but it does not always yield positive results. When studying on online markets, if transparent communication fails, researchers may need to adopt the fictitious position of an interested buyer to get information on the sellers. In such case, ethical considerations regarding deception must be addressed.

After a successful first contact, researchers must inform participants about the purpose of the research, specifying who will participate and be able to access the data collected; how the data will be treated and anonymized; what tools will be used to contact them; and an estimate of the time needed to complete and review the interview (Seidman, 2019). It would be wise to use specific devices to perform this type of research and avoid opening files sent by participants, as they can easily hide malware in them. This can be a problem if participants send their own responses in, for example, a Word or PDF file. In these cases, it would be better to have them send the responses in plain text in the body of the email. Researchers must also inform participants of their right to withdraw from the project and to have their data deleted, and of the possible risks the research might entail.

1.4 Techniques employed

Below we describe our experience in applying seven techniques to research on cybercriminals, addressing questions such as what the technique involves, what kind of measures it collects, how time consuming it is, what type of insights it provides, what kind of samples it usually allows to collect, what skills it needs, and whether it is intrusive or not. We close this section with a structured overview of the characteristics of the techniques.

1.4.1 Interviews

Interviews—whether unstructured, semi-structured, o structured—serve to gather in-depth information about the perceptions of respondents on a particular topic. Researchers can interview cybercriminals offline and online (Hutchings and Holt, 2018). We have reached hackers both ways and we found no magic recipe for them to accept an interview. In our experience, the most important factor is usually trust, either built over time or fostered by a referral. In the case of online interviews, the use of encrypted communication channels can also help convince respondents. Note that cybercriminals may make statements that are not verifiable, try to impress the interviewer by exaggerating their activities or downplaying them, or agree with the interviewer to have an easy and accommodating conversation rather than a challenging one. Interviews are time-consuming, especially when respondents are hard-to-reach or have limited time.

Usually, offline interviews take less time and are richer than online interviews because of the additional information that emerges from the conversation (e.g. body language, tone of voice). Offline interviews with hackers usually take between three and five hours. In contrast, online interviews with hacktivists can extend over days or even weeks in a series of short sessions of about 30 minutes due the time it takes to type and the availability of respondents (note that interviewees may multitask, or live in a different time zone) (Romagna & Leukfeldt, 2022). Such breaks interrupt the conversation, but they also allow the interviewer to verify responses, ask additional questions or seek clarification, and give respondents more time to reflect on their answers too (O'Connor and Madge, 2017). In online interviews, respondents may get lazy and end up with simple answers. This is often the case over email, but live chats allow for much more depth. For example, since respondents do not have to type in their response when exchanging audio messages through instant messaging applications such as Signal, Telegram, and WhatsApp, the information they provide is more detailed—similar to that collected in offline interviews. Audio files also allow to evaluate the tone of voice and emotions of respondents (e.g. irony, anger, sadness). The downside is that it takes a long time to listen to and transcribe the audio. Although software approximates automatic transcription, it is often not accurate and requires revision. To ensure privacy and confidentiality, software must be secure, validated and reliable, so it is generally not safe to use free versions.

Interviewers should be friendly and open, and be willing to humor the interviewee. While it is necessary to keep control of the conversation, some digressions should be allowed. These help to strengthen the bond with the respondent, especially since it is often not possible to have any face-to-face or even visual contact (Salmons, 2014). A certain knowledge of the field helps to follow the conversation, especially when the language becomes particularly technical, but it is also helpful to ask for clarification (Seidman, 2019). While cybercriminals are not always happy to explain certain things—such as the techniques and tools they use, the exact number of people involved in an operation, their actual location, and the ways they meet other cybercriminals and share information—they may like the idea of teaching someone else certain concepts or skills or simply directing the interviewer to the right information.

Note that it is usually not possible to generalize interview results. Our samples are usually around 25 respondents, but even though hackers are hard-to-reach populations, such figures are not sufficient to draw general conclusions. In such cases, we apply the saturation principle: once the answers become more and more similar and hardly anything new is added, one can assume that other respondents would be in the same line of thinking (Seidman, 2019).

1.4.2 Questionnaires

Questionnaires are measurement instruments used to collect information from respondents in a standardized manner, and can be administered offline or online. The advantage of the online route is that reaching a large sample is cost-effective. For this purpose, researchers often resort to companies that curate panels of respondents, or to online platforms where the target population interacts. In both cases, the representativeness of the sample is often problematic

due to self-selection bias. In addition, researchers should keep in mind that often the most interesting populations (e.g. hackers) are also the least accessible. Sometimes it can be useful to offer an incentive for participation. For example, Weulen Kranenbarg (2021) offered a €50 incentive to 928 cybercrime suspects to report their cyber offending in a survey and, after two reminders, achieved a response rate of 28.9%—which was higher than the 16.1% response rate she obtained from traditional crime suspects. Together with interviews, questionnaires and surveys are the data collection method par excellence in the social sciences and as such have been used extensively in cybercrime research, mainly to collect subjective measures of behavior such as self-reported offending (e.g. Marcum et al., 2014), but in some cases also objective ones such as IT skills (e.g. Weulen Kranenbarg et al., 2021).

The difference between the two is that subjective measures rely on the perception of the respondents, while objective measures capture their performance. While subjective measures allow to collect, for example, what respondents think about what their behavior, knowledge or skills are, objective measures can be used to measure their actual dimension. This is an important distinction, as a recent systematic review and meta-analysis shows that subjective online behavioral measures are only moderately related to objective ones (Parry et al., 2021). The validity of objective measures is therefore considered better.

Some of the most common subjective measures refer to the prevalence of behaviors such as offending or victimization in a given period of time, and usually follow the formula: "In the last 12 months, how often have you performed/experienced [behavior]?" or "Have you ever performed/experienced [behavior]?". Regarding objective measures, for example, researchers developed a 10-item questionnaire in collaboration with the Dutch National Police to measure the objective IT skills of a sample of cyber-dependent crime suspects (Weulen Kranenbarg et al., 2021). We captured the objective online behavior of a representative sample from the Netherlands using an online questionnaire in which respondents were presented with a series of cyber risky situations to resolve (van 't Hoff-de Goede et al., 2019). This strategy served to measure the strength of passwords used by respondents, software downloads, clicks on pop-up windows, personal information shared online, and interactions with email attachments and hyperlinks.

1.4.3 Monitoring software

Monitoring software is a broad term used to encompass everything from session-only tracking mechanisms, to video recording, to fingerprinting methods that serve to capture the objective activity of a user on a computer (for reviews see Bujlow et al., 2017; Fourie and Bothma, 2007). Monitoring software can capture all kinds of data from users, such as the activities they perform online and locally (e.g. websites visited, programs run), when they do so, and their keystrokes while at it. The insights it provides are unique.

Research designs that collect measurements with monitoring software generally require infrastructure such as computers or computer labs in addition to the software itself—which is usually paid for. The installation and maintenance of this setup requires IT skills, so we

recommend collaborating with computer scientists. Data collected through monitoring software may require complex preprocessing to prepare it for analysis if it is stored in unstructured or semi-structured formats such as plain text. So in these cases data science skills are a good asset.

Combined with cybersecurity educational exercises, such as capture the flag (CTF) (Švábenský et al., 2021), monitoring software may reveal insights into the decision-making process of individuals with high IT skills when faced with cybersecurity challenges similar to those encountered by hackers in the real world (Moneva et al., 2022c). This is an innovative method for researchers who want to collect objective online behavioral measures in cybercrime contexts. However, preparing CTFs is often a costly task that requires to set a lab up, recruit participants, design a cybersecurity exercise, and collect the data generated by the participants. This means that, depending on available resources, data collection can take several months. Good planning is therefore essential. Samples collected with this design are usually small as they are limited by the number of computers available with the monitoring software. For example, the computer lab we used at The Hague University of Applied Sciences had two rooms, with 26 and 28 computers. We recruited 72 participants for seven data collection sessions over two days, each hosting between three and 14 participants (Moneva et al., 2022c). As for the type of participants that can be recruited through CTFs, the existing IT infrastructure at university departments, along with the pool of computer security or software engineering students that many have, makes it practical to start with these convenience samples. Perhaps more valuable samples include IT security experts, white hat hackers and, ideally, black hat hackers. Because of the skills of the participants, it is important to take security measures seriously and use controlled online environments for the exercises in case participants attack the IT infrastructure. Virtual machines provide an additional layer of protection that can prove invaluable.

1.4.4 Online ads as honeypots

Criminologists often use honeypots to better understand cybercrime (Perkins and Howell, 2021). Honeypots are computer tools designed to attract Internet users to interact with them and collect the data this interaction generates (Spitzner, 2002). Honeypots can take many forms: computer networks, websites, social media accounts, or online ads, among many others.

One of the main advantages of honeypots is that they can capture objective online behavior. For example, a honeypot network can capture trespassing attempts (Maimon et al., 2014), and a honeypot email account can capture communications with offenders (Maimon et al., 2020). And since honeypots are generally released in the wild, they tend to capture large volumes of interactions, which usually translates into large samples. Depending on the environment where they are released, honeypots will attract a different population: a fake barely-legal pornography website (Prichard et al., 2021) will not attract the same users as online ads to prevent DDoS attacks on the gaming industry (Moneva et al., 2022a), nor the same as

money mule recruitment messages (Bekkers and Leukfeldt, 2022). Researchers need to think in advance which population they want to attract before choosing the most suitable honeypot.

The measures that a honeypot collects vary depending on its design. This means that, with the appropriate skills, it is possible to design a honeypot that collects custom measures. While creating a honeypot can require extensive IT skills, using third-party infrastructure or software is often less demanding in this sense. When designing and using honeypots, it is important to consider the activity of bots online. Without proper filters, bots can alter the data collected and thus affect analysis (Perkins and Howell, 2021; see also Vetterl, 2020). For example, a repeated count of intrusion attempts may be due to bot activity and not necessarily to humans. It is not always necessary, however, to build a honeypot from scratch; it is also possible to use existing tools as honeypots. For example, we used the advertisement tools from Google and Meta to deliver targeted online ads to populations at risk of getting involved into cybercrime (Bekkers et al., 2022; Moneva et al., 2022a). These solutions allowed us to trade the resources that setting up the infrastructure would have required in exchange for using a set of predefined measurements. If the predefined measures happen to be the ones that the researchers need—as was the case—this is not a problem. Researchers using third-party tools must accept their terms and conditions of use which may be relevant to data processing and privacy issues. For example, Google must adhere to the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016) when collecting and processing user data from the Netherlands.

1.4.5 Analysis of secondary data (Zone-H)

Secondary data are those collected by someone other than the researchers who will use them. This means that researchers have no control over the method of collection or the information contained in them (Bookstaver, 2021). Their analysis therefore constitutes a non-intrusive research technique. When using secondary data, it is important to contact the data collectors to gain insights; we in fact discovered some particularities in doing so.

One of the most popular sources of secondary data on hacking is the Zone-H Defacement Archive [1] (see Romagna and Van den Hout, 2017). In Zone-H, alleged hackers—or groups of hackers—self-report their defacement activity under a nickname, providing evidence via the URL of the defaced website and selecting from a drop-down menu the method of intrusion used and their motivation. Researchers can contact the database administrators to purchase a data dump with the desired coverage (e.g. temporal, territorial)—the cost of which varies according to the request—and analyze it to answer their research questions. In this way it is possible to access millions of hacking records. Once received, data require little cleaning and the variables they contain are intuitive, making them easy data to work with requiring standard data analysis skills. We used Zone-H data to, for example, test repeat victimization premises (Moneva et al., 2022b), the routine activities approach and target suitability (Holt et al., 2020), and identify defacer trajectories (van de Weijer et al., 2021).

[1] See http://www.zone-h.org/. Last accessed on 3 March 2023.

However, the Zone-H data have a particular characteristics that is important to note. In order to protect certain domains from being repeatedly targeted as a result of appearing on the Zone-H public listing, the administrators imposed a one-year restriction on re-registering a defaced domain, thus altering the statistical distribution of defacements (Moneva et al., 2022b). The second, more obvious, is that the time stamp of each observation does not correspond to the time at which the defacement occurred, but corresponds to its reporting and recording, which usually follows a verification process of one or two weeks. Both aspects have obvious limitations for data analysis and modeling that are important to acknowledge.

1.4.6 Qualitative analysis of criminal investigations

Criminal investigations by the police inform criminal trials and have been used to shed light on cybercriminals and their activities (Leukfeldt and Kleemans, 2021). These police investigations provide unique in-depth knowledge because of the use of intrusive investigative methods such as wiretaps and IP taps, observations, undercover policing, and house searches.

The Dutch Organized Crime Monitor was established in the mid-90s in the Netherlands to enable academic research into organized crime. The monitor includes closed police cases on a broad cross-section of organized crime (see Kleemans, 2014), whose information can be systematically analyzed using checklists (e.g. Kruisbergen et al., 2019; Leukfeldt and Holt, 2022). The checklists we used covered: 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, expenditures, money laundering, and seized assets; the judicial procedure and verdict; and the evaluation (i.e. lessons learned, new insights, prevention opportunities, new developments, and effectiveness of policing strategies). Unfortunately, not all countries grant academics access to police cases. Alternatively, cases can also be reconstructed based on the use of publicly available court cases and structured interviews with police officers, prosecutors, and other relevant people (Leukfeldt et al., 2017c). While this does not provide researchers with the raw data (e.g. transcripts of taped conversations or chat logs), interviews with investigators—who in some cases have been investigating criminal groups for years—provide an in-depth understanding of the criminal networks and their members.

Case reconstructions have some distinct advantages over the analysis of police investigations. First, police cases do not always contain all relevant information about criminal networks, as they focus on collecting evidence. Relevant knowledge about, for example, the social ties or offender convergence settings may not be part of the police file, but is often known to the respondents. The opposite is also true: police cases may contain sensitive information that is not always of interest for academic purposes. Finally, interviews make it possible to include the most recent cases, as 'closing' criminal investigations can take long.

1.4.7 Overview

Table 1 provides a summary overview of the techniques presented above.

Table 1. Overview of the techniques employed

Technique	Measures collected	Time investment	Sample size	Skills required	Intrusive	Insights
Interviews	Subjective	High	Small	Qualitative	Yes	In-depth knowledge
Questionnaires	Objective and subjective	Low	Medium to large	Quantitative, qualitative	Yes	Standardized measures
Monitoring software	Objective	High	Small to medium	IT, quantitative	Yes	Interdisciplinary work, requires infrastructure
Online ads as honeypots	Objective	Medium	Large	IT, quantitative	Yes	Requires infrastructure
Analysis of secondary data (Zone-H)	Subjective	Low	Large	Quantitative, qualitative	No	Verified by admins, mirrored defacements
Qualitative analysis of criminal investigations	Objective and subjective	High	Small to medium	Qualitative	No	Police investigations, court documents, expert knowledge

1.5 Ethical and emotional aspects

This section focuses on the ethical and emotional aspects on which we have been advised by criminological ethics committees. For the general ethical challenges of cybercrime research (i.e. privacy and other legal issues, informed consent, protecting the participants and researchers), see (Castro-Toledo and Miró-Llinares, 2021). In our experience, compared to generic ethics committees, a criminological ethics committee is likely to be more aware of the complexities of criminological research and understand the use of more intrusive methodologies when justified. We recommend consulting these specialized committees.

1.5.1 Preserving anonymity and confidentiality

Sometimes it can be tempting to use the nicknames that cybercriminals use on social media, forums, or marketplaces to apply an additional layer of reality to our research. We may also deem it enlightening to use verbatim quotes from the contents they publish publicly or share privately. Since the nicknames are not real names, it may give the impression that the subjects already enjoy sufficient anonymity. However, some people use the same nicknames across different platforms—and the same applies to the people with whom they communicate—which can be used to triangulate information available online to reduce or eliminate their anonymity. To ensure the anonymity of the subjects, nicknames should always be anonymized and their messages paraphrased (Hutchings and Holt, 2018). Note that this is a two-way street. Researchers may also expose their own safety by revealing their identity to participants, which

creates various tensions that may affect the personal and professional sphere (Lavorgna and Sugiura, 2022).

In addition, if we monitor the activity of cybercriminals or collect information they shared non-publicly, we may pick up sensitive information in the process, such as real names, email accounts, or passwords. As soon as this information is detected, it should be deleted (Hutchings and Holt, 2018). Researchers must ensure that the information provided by the participant is not leaked and take into consideration details such as isolation of space, encryption of files, access to workspaces and computers, and data storage. These are just two examples—each setups require specific attention.

1.5.2 Identifying minors

Sometimes it can be difficult to determine if a person is underage. This is much more difficult online. In ideal circumstances, researchers will try to obtain proof of age through some official document. This is possible when, for example, subjects have gone through the justice system, as the police will collect such information. However, when contacting cybercriminals in the wild this is highly problematic. It is likely that subjects will never reveal their true age or will reveal a false age. Some subjects may not take kindly to a request that their parents or legal guardians sign an informed consent form in their place, which may result in the loss of a valuable and often already scarce sample. When in doubt, investigators will be faced with the dilemma of whether to proceed with the research at all. In such cases, we recommend that researchers always treat subjects as minors.

1.5.3 Deceiving cybercriminals with honeypots

Researchers deploy honeypots to collect objective behavioral data from online users. For honeypots to be effective, they must mimic computer systems such as networks, websites, or ads, which are of interest to the target population (e.g. cybercriminals). This often involves deception and data collection without consent, which raises ethical concerns (Castro-Toledo and Gómez-Bellvís, in press). The reason researchers continue to resort to this design is that warning participants that the honeypot is not a real system and asking for their consent to collect their data would invalidate the research design. No cybercriminal would interact with the honeypot, so researchers would not be able to study their behavior in a realistic online scenario. This would have serious consequences for cybercrime prevention and cybersecurity, as the behavioral measures collected would be inaccurate and the conclusions drawn, therefore, flawed.

Faced with this ethical dilemma, Castro-Toledo and Gómez-Bellvís (in press) propose three conditions for the use of honeypots in online deviance research: that they serve to address a problem of public interest like cybercrime prevention, that there is no methodology better suited to answer the research question, and that the honeypot is fully simulated. Although we believe that cybercrime researchers usually meet all three conditions, it is important to always keep them in mind.

1.5.4 Witnessing serious cybercrimes

During the course of the research, researchers may access websites, forums, or marketplaces where cybercriminals commit crimes or engage in deviant behaviors. Often, finding these sites is easier than it seems and there is no need to visit the dark web. In most cases, depending on the objective of the investigation, such crimes will be financially motivated and will consist of transactions of information (e.g. personal data, software) and objects (e.g. drugs, weapons) in exchange for money. In some cases, researchers may witness situations that affect them emotionally, such the trade of child sexual exploitation material (CSEM). We recommend that researchers seek psychological help if they expect to be confronted with these situations or if they have been affected by them.

Researchers may also consider reporting certain crimes to the police (Rauhala and Kalokairinou, 2021). Sometimes respondents talk about crimes they have committed or will commit. We advise to explicitly ask respondents not to disclose or discuss possible illegal activities they plan in the future (see also Hutchings and Holt, 2018).

1.5.5 Keeping a professional distance

One risk that researchers may encounter, especially in long and emotionally demanding projects, is the risk of going native and getting too caught up in the dynamics of the population under study. Especially when interviews go on for a long time, researchers may develop an unexpected friendship with participants. In such cases, researchers should be aware that any new information obtained could be biased. Participants may even forget that they are part of a study and provide information in confidence. Should researchers wish to obtain new information for their study from their now-friend, they should keep a professional distance. Sometimes it is also difficult to detach from these relationships, especially when the respondent is strongly attached to them. In such situations, it is necessary to proceed with a constant but slow process of distancing, to avoid hurting the respondent's feelings. This process must be carefully calculated, especially in the case of cybercriminals, because retaliation can be dangerous. However, if researchers and participants agree to maintain contact, participants can become a source of information and gatekeepers for future research. Clear communication is key to acting appropriately if research activity resumes.

1.6 Lessons learned and methodological perspectives

1.6.1 Lessons learned

Interviews. Hackers are a particular type of cybercriminals who have a specific perception of themselves and their activities. They often follow a cultural and ethical code that may conflict with that of society, and justify their actions by claiming to pursue a greater purpose (e.g. fight enemies, help people). They may describe their activities as a good challenge or just plain fun, without trying to avoid judgment for their questionable actions. Once trust is established, hackers can be friendly and helpful, fun and open to dialogue, often willing to provide answers

and chat, guiding the investigator through the intricacies of their activities. They also claim to be busy people and sometimes it is necessary to send reminders for a meeting or an interview, but—in general—they have proven to be polite and even friendly. In fact, hackers are often available at unexpected hours, as many are engaged in hacking as a sideline and therefore only have time during evening hours or on weekends.

Hackers can also be extremely suspicious, so it is advisable to communicate with them openly, using mutually trusted tools that cannot be used as attack vectors. Therefore, sending attachments via email or chat is not something hackers like to do. Lying about or masking part of your research is also not advisable. Researchers should also expect a thorough search of their digital persona, as hackers will likely try to verify their identity. Affiliations with certain institutions, such as law enforcement, can cause problems and keep respondents at bay, and should always be clearly introduced at the beginning of the research. Note that, depending on the activities they engage in, like hacktivism or crime, some hackers will be more willing to talk than others.

Questionnaires. Adequately motivating respondents is essential to count on their cooperation in filling out questionnaires reliably. For example, IT security students may value extra points on an assignment more than a modest amount of money as compensation. Likewise, if any IT savvy respondents find that our IT skills module contains errors or is inadequate to measure their skill level, they may also perceive that the researchers lack expertise to conduct the study, which may in turn diminish their legitimacy in the eyes of the respondents. Despite possible incentives offered for their participation in the research, some respondents will lack the motivation or patience to complete the often tedious questionnaires that academics prepare. In these cases respondents might rush through the items by selecting random options or skipping entire questions. These are the speeders. This is why it is always advisable to collect the response times of the respondents to detect speeders in case all our efforts to motivate them were in vain.

Online questionnaires are susceptible to technical problems such as loss of Internet connection or questions not displaying correctly. These problems are difficult to spot when admnistered remotely and will only be detected in the data (if at all) when it is too late to solve them. Whenever possible, we advise that the researchers accompany the respondents during the exercise. If this is not possible, simply acknowledge that this can happen.

Monitoring software. Setting up computer labs with monitoring software is an arduous task—and, to a lesser extent, so is setting up individual workstations. These labs are often guided by strict cybersecurity policies to protect the institutions that host them. The technicians in charge of running these labs are the gatekeepers of their security. They are the ones who best know the equipment and the ins and outs of the system. These technicians may be reluctant to install new software on your machines, and may require to verify that they do not possess any harm. In addition, computer labs are often in high demand, usually for educational exercises, so it is advisable to reserve a time slot for the study well in advance. Some labs are open to

students, so it is important to control access to prevent any unwary person from interfering with the research.

Despite the invaluable help of the technicians, considering the complex setup required for this type of research, it is very likely that if something can go wrong, it will go wrong. We recommend being thorough and conducting pilot studies that test each stage of the research. It may also be wise to consider several data collection rounds rather than concentrating all participants in a single session in case something does go wrong (e.g. someone is late, changes workstations, or cheats).

Online ads as honeypots. Researchers often insist on building their own tools to collect research data. But this effort does not always pay off. There are data collection tools out there, or data themselves, that can be useful in cybercrime research. Sometimes academics are reluctant to use tools designed by third parties for transparency reasons; if we do not know exactly how they work we reject them. But there are tools that have extensive documentation on how they work that may not be completely comprehensive, but may be comprehensive enough. We believe that these technologies should be embraced rather than rejected, especially if they are already being used by stakeholders or policy makers, as in the case of Google Ads. In such cases, researchers can not only take advantage of their usefulness, but also act as impartial evaluators. Our thorough research may help detect flaws in their design that—at worst—can inform their users, or features that—at best—enable future research.

When using a new technology, it is important to understand it thoroughly. In addition to any documentation available, commercial software often has support staff that can answer many questions. Alternatively, researchers can hire third parties who are experts in such technologies to handle data collection on their behalf. While this may sometimes be the only option, we recommend that researchers maintain close contact with these teams and supervise them in the process, as the experts may know the technology, but probably not the details of the research design. For example, while it is possible to collect a lot of data with Google Ads, it may be necessary to apply some filters; the goal is not to get a lot of data, but to get the right data. Google Ads' interface can be overwhelming for new users, so expert help in such cases may prove useful.

Analysis of secondary data (Zone-H). Often the secondary data is clean and ready to use. The best datasets come with detailed codebooks. But these datasets are scarce. In some cases, the data also holds secrets. For example, the name of a variable may suggest that it measures one thing, but it actually measures something else; the data collection process may have particularities that are not explained in detail anywhere, but are crucial for interpreting the data. Contacting the Zone-H administrators was extremely useful in our research, as they had insights about the data that were not reflected in the documentation and had not been reported in previous research. We always recommend going to the source in case of doubts, to avoid misinterpretations. In the end, data without context is meaningless.

Qualitative analysis of criminal investigations. Police cases offer unique data that provides insight into a criminal world which is normally hidden. Because of their special

investigative powers, law enforcement agencies are able to observe criminal activities, log online and offline conversations and analyze material on seized computers and servers. There is no doubt that these insights are hard to get using other methods. Besides some obvious limitations like bias in the type of offenders and crimes, and the limited number of cases available, time is an important factor when analyzing police data. Firstly, strict procedures lengthen the access time for police data. In the Netherlands, these procedures can take between three to nine months, depending on how many applications there are. And applying does not guarantee access. Second, once access is granted, it takes time to identify relevant cases (usually archived in different cities all over the country) and it may take days or weeks to analyze a single case, depending on the length of the investigation or the special powers used. An alternative we used over the past decade are 'case reconstructions' instead of analyzing actual police data. Cases are identified based on news report and interviews with law enforcement agencies. Each case has a district attorney and one or two law enforcement agents responsible for large parts of the criminal investigation. Interviewing these persons in combination with analyzing publicly available documents, like court documents and press releases, also provides relevant information about criminal networks and their members.

1.6.2 Methodological perspectives

Innovation and good old tradition. Innovation is what advances science, but tradition is what sustains it. New methodologies and analysis techniques open the door to new perspectives and interpretations of reality, but we cannot abandon the valuable traditional methods that produce reliable knowledge. It may seem that, when it comes to investigating cybercriminals, web scraping and big data are the only options for conducting research. Not only is this not true, but it can produce a distorted picture of reality. For example, the insights that investigators obtain from big scraped forum data can show how buyers and sellers relate to each other in an illicit cybercrime market ecosystem, but without examining the criminal investigations that law enforcement conducts, we will only be exposed to the information that cybercriminals share and not what they hide. Similarly, experiments with IoT honeypots may reveal new patterns of behavior of previously unknown hackers, but it will be very difficult to understand their decision making process with respect to trespassing if we do not interview them. Inevitably, strong methodological preferences create biases and knowledge gaps that must be compensated for. Therefore, we believe that for the field to thrive, it is necessary to combine innovative and traditional research. This does not mean that every researcher should do both, but that there should be specialists in both.

Interdisciplinarity. That cybercrime research benefits from the connections established between different disciplines of the social and computer sciences is something that has been recurrently acknowledged in the scientific literature (Holt, 2017; Maimon and Louderback, 2019). To draw a complete picture of cybercriminals, researchers must be able to grasp their human dimension and understand the technology they use, which immediately involves aspects of criminology, psychology, sociology, IT security, and engineering, among others. Some of

the most ambitious research designs, like those involving computer labs and monitoring software, and honeypots, are interdisciplinary by definition and require interdisciplinary teams to unfold their full potential. In these scenarios, criminologists may benefit from collaborating with software engineers to develop software to collect data and with IT security researchers to interpret the modus operandi of cybercriminals. Considering the current state of the field, it is likely that many of the innovations in cybercrime research will come from interdisciplinary collaborations that apply knowledge from one discipline to the field of study of another.

Objective measures of online behavior. To obtain insights about cybercriminals, due to the difficulty of accessing trustworthy information, researchers have largely relied on self-reported data, usually through interviews and questionnaires. These data have helped propel the field forward by providing important insights into why and how cybercriminals engage in cybercrime, as well as what the risk factors are for such behavior. However, recent synthesis research has shown that self-reported or subjective measures of online behavior are only moderately correlated with objective measures (Parry et al., 2021). To gain more accurate insights on cyber offending, it is necessary to add objective measures to our repertoire, like questionnaires, monitoring software, honeypots, and criminal investigations, observation and web scraping.

A plea for replicability and reproducibility. In recent decades, researchers noted a replication crisis in psychology that likely extends to criminology, and the social sciences at large (Pridemore et al., 2018). Some practices may improve replicability, such as "increasing sample size, preregistering studies, improving rigor and transparency, sharing materials and primary data, conducting replications, and enhancing error detection and correction" (Nosek et al., 2022, p. 735). It may seem that these practices only concern quantitative research designs, but they also apply to qualitative ones. Although, for example, reproducing the transcript of an interview with a cybercriminal is virtually impossible, it can be argued that it is still possible to increase the replicability of qualitative research by following some of the practices listed above. For example, one can increase the number of interviewees, pre-register research questions and analysis techniques, share anonymized transcripts, and repeat interviews on a new sample. Transparency and rigor in the interpretation of transcripts can also aid in error detection and correction. This discussion transcends research on cybercriminals, but certainly affects it. We believe that research institutions should promote a culture of change among researchers to adopt these good and open science practices to build a strong field on reliable evidence that gains the trust of practitioners, professionals, and policy makers.

References

Bekkers, L.M.J., Leukfeldt, E.R., 2022. Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime. Deviant Behavior 1–17. https://doi.org/10.1080/01639625.2022.2073298

Bekkers, L.M.J., Moneva, A., Leukfeldt, E.R., 2022. Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. Journal of Experimental Criminology 1–20. https://doi.org/10.1007/s11292-022-09537-7

Bookstaver, M., 2021. Secondary Data Analysis, in: Barnes, J.C., Forde, D.R. (Eds.), The Encyclopedia of Research Methods in Criminology and Criminal Justice. Wiley, pp. 531–534. https://doi.org/10.1002/9781119111931.ch107

Bujlow, T., Carela-Espanol, V., Lee, B.-R., Barlet-Ros, P., 2017. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. Proc. IEEE 105, 1476–1510. https://doi.org/10.1109/JPROC.2016.2637878

Castro-Toledo, F.J., Gómez-Bellvís, A.B., in press. Ethics of covert surveillance in online deviance research using honeypots, in: Graham, R., Humer, S.G., Lee, C.S., Nagy, V. (Eds.), Routledge International Handbook of Online Deviance. Routledge, Taylor & Francis Group.

Castro-Toledo, F.J., Miró-Llinares, F., 2021. Researching Cybercrime in the European Union: Asking the Right Ethics Questions, in: Lavorgna, A., Holt, T.J. (Eds.), Researching Cybercrimes. Springer International Publishing, Cham, pp. 327–345. https://doi.org/10.1007/978-3-030-74837-1_16

Chua, Y.T., Holt, T.J., 2016. A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. Victims & Offenders 11, 534–555. https://doi.org/10.1080/15564886.2015.1121944

Del-Real, C., Rodriguez Mesa, M.J., 2022. From black to white: The regulation of ethical hacking in Spain. Information & Communications Technology Law.

European Parliament, Council of the European Union, 2016. General Data Protection Regulation. Official Journal of the European Union 59, 1–88.

Fourie, I., Bothma, T., 2007. Information seeking: an overview of web tracking and the criteria for tracking software. Aslib Proceedings 59, 264–284. https://doi.org/10.1108/00012530710752052

Holt, T.J., 2020. Computer Hacking and the Hacker Subculture, in: Holt, T.J., Bossler, A.M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer International Publishing, Cham, pp. 725–742. https://doi.org/10.1007/978-3-319-78440-3_31

Holt, T.J., 2017. Cybercrime through an interdisciplinary lens, Routledge studies in crime and society. Routledge, Taylor & Francis Group, London ; New York.

Holt, T.J., 2007. Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. Deviant Behavior 28, 171–198. https://doi.org/10.1080/01639620601131065

Holt, T.J., Bossler, A.M., 2016. Cybercrime in progress: theory and prevention of technology-enabled offenses, First Edition. ed, Crime Science Series ; 17. Routledge, London; New York.

Holt, T.J., Bossler, A.M., May, D.C., 2012. Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. Am J Crim Just 37, 378–395. https://doi.org/10.1007/s12103-011-9117-3

Holt, T.J., Leukfeldt, E.R., van de Weijer, S.G.A., 2020. An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites.

Criminal Justice and Behavior 47, 487–505. https://doi.org/10.1177/0093854819900322
Hutchings, A., Holt, T.J., 2018. Interviewing Cybercrime Offenders.
Internet Crime Complaint Center, 2021. 2021 Internet Crime Report. Federal Bureau of Investigation.
Jordan, T., 2017. A genealogy of hacking. Convergence 23, 528–544. https://doi.org/10.1177/1354856516640710
Kleemans, E.R., 2014. Organized Crime Research: Challenging assumptions and informing policy, in: Cockbain, E., Knutsson, J. (Eds.), Applied Police Research. Routledge, pp. 57–67. https://doi.org/10.4324/9781315815305
Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R., Roks, R.A., 2019. Money talks money laundering choices of organized crime offenders in a digital age. Journal of Crime and Justice 42, 569–581. https://doi.org/10.1080/0735648X.2019.1692420
Lavorgna, A., Holt, T.J. (Eds.), 2021. Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-74837-1
Leukfeldt, E.R., Holt, T.J., 2022. Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. Computers in Human Behavior 126, 106979. https://doi.org/10.1016/j.chb.2021.106979
Leukfeldt, E.R., Kleemans, E.R., 2021. Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime, in: Lavorgna, A., Holt, T.J. (Eds.), Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches. Springer International Publishing, Cham, pp. 127–144. https://doi.org/10.1007/978-3-030-74837-1
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, 704–722. https://doi.org/10.1093/bjc/azw009
Leukfeldt, E.R., Kleemans, E.R., Stol, W.P., 2017b. The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. American Behavioral Scientist 61, 1387–1402. https://doi.org/10.1177/0002764217734267
Leukfeldt, E.R., Kleemans, E.R., Stol, W.P., 2017c. Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. Crime Law Soc Change 67, 39–53. https://doi.org/10.1007/s10611-016-9663-1
Levy, S., 1984. Hackers: heroes of the computer revolution, 1st ed. ed. Anchor Press/Doubleday, Garden City, N.Y.
Maimon, D., Alper, M., Sobesto, B., Cukier, M., 2014. Restrictive deterrent effects of a warning banner in an attacked computer system. Criminology 52, 33–59. https://doi.org/10.1111/1745-9125.12028
Maimon, D., Howell, C.J., Moloney, M., Park, Y.S., 2020. An Examination of Email Fraudsters' Modus Operandi. Crime & Delinquency 001112872096850. https://doi.org/10.1177/0011128720968504
Maimon, D., Louderback, E.R., 2019. Cyber-Dependent Crimes: An Interdisciplinary Review. Annual Review of Criminology 2, 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057
Marcum, C.D., Higgins, G.E., Ricketts, M.L., Wolfe, S.E., 2014. Hacking in High School: Cybercrime Perpetration by Juveniles. Deviant Behavior 35, 581–591. https://doi.org/10.1080/01639625.2013.867721
McGuire, M.R., 2020. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime, in: Leukfeldt, E.R., Holt, T.J. (Eds.), The Human Factor of

Cybercrime, Routledge Studies in Crime and Society. Rutledge, London; New York, pp. 3–28.
McGuire, M.R., Dowling, S., 2013. Cyber crime: a review of the evidence (No. 75). Home Office, United Kingdom.
Miró-Llinares, F., Johnson, S.D., 2018. Cybercrime and Place: Applying Environmental Criminology to Crimes in Cyberspace, in: Bruinsma, G.J.N., Johnson, S.D. (Eds.), The Oxford Handbook of Environmental Criminology. Oxford University Press, Oxford, pp. 883–906. https://doi.org/10.1093/oxfordhb/9780190279707.013.39
Moneva, A., 2020. Cyber Places, Crime Patterns, and Cybercrime Prevention: An Environmental Criminology and Crime Analysis approach through Data Science (Doctoral thesis). Miguel Hernandez University, Elche.
Moneva, A., Leukfeldt, E.R., Klijnsoon, W., 2022a. Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners. J Exp Criminol. https://doi.org/10.1007/s11292-022-09504-2
Moneva, A., Leukfeldt, E.R., van de Weijer, S.G.A., Miró-Llinares, F., 2022b. Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. Computers in Human Behavior 126. https://doi.org/10.1016/j.chb.2021.106984
Moneva, A., Ruiter, S., Meinsma, D., 2022c. Hacker Mobility in Cyberspace and the Least Effort Principle: Examining Efficiency in the Journey to Cybercrime. https://doi.org/10.17605/OSF.IO/UFDP8
Nosek, B.A., Hardwicke, T.E., Moshontz, H., Allard, A., Corker, K.S., Dreber, A., Fidler, F., Hilgard, J., Kline Struhl, M., Nuijten, M.B., Rohrer, J.M., Romero, F., Scheel, A.M., Scherer, L.D., Schönbrodt, F.D., Vazire, S., 2022. Replicability, Robustness, and Reproducibility in Psychological Science. Annu. Rev. Psychol. 73, 719–748. https://doi.org/10.1146/annurev-psych-020821-114157
O'Connor, H., Madge, C., 2017. Online Interviewing, in: The SAGE Handbook of Online Research Methods. SAGE Publications Ltd, London, pp. 416–434. https://doi.org/10.4135/9781473957992.n24
Parry, D.A., Davidson, B.I., Sewall, C.J.R., Fisher, J.T., Mieczkowski, H., Quintana, D.S., 2021. A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use. Nat Hum Behav 5, 1535–1547. https://doi.org/10.1038/s41562-021-01117-5
Perkins, R.C., Howell, C.J., 2021. Honeypots for Cybercrime Research, in: Lavorgna, A., Holt, T.J. (Eds.), Researching Cybercrimes. Springer International Publishing, Cham, pp. 233–261. https://doi.org/10.1007/978-3-030-74837-1_12
Prichard, J., Wortley, R., Watters, P.A., Spiranovic, C., Hunn, C., Krone, T., 2021. Effects of Automated Messages on Internet Users Attempting to Access "Barely Legal" Pornography. Sex Abuse 107906322110138. https://doi.org/10.1177/10790632211013809
Pridemore, W.A., Makel, M.C., Plucker, J.A., 2018. Replication in Criminology and the Social Sciences. Annual Review of Criminology 1, 19–38. https://doi.org/10.1146/annurev-criminol-032317-091849
Rauhala, M., Kalokairinou, L., 2021. Ethics in Social Science and Humanities. European Commission, Belgium.
Romagna, M., 2020. Hacktivism: Conceptualization, Techniques, and Historical View, in: Holt, T.J., Bossler, A.M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer International Publishing, Cham, pp. 1–27. https://doi.org/10.1007/978-3-319-90307-1_34-1

Romagna, M., Leukfeldt, E.R., in press. Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. Crime and Justice.
Romagna, M., Van den Hout, N.J., 2017. Hacktivism and website defacement: Motivations, capabilities and potential threats. Presented at the Virus Bulletin Conference (VB2017), Madrid, pp. 1–11.
Salmons, J., 2014. Qualitative online interviews: strategies, design, and skills, Second Edition. ed. SAGE, Los Angeles.
Schell, B.H., Dodge, J.L., 2002. The hacking of America: who's doing it, why, and how. Quorum Books, Westport, CT.
Schiks, J.A.M., van 't Hoff-de Goede, M.S., Leukfeldt, E.R., 2021. Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right. Sdu uitgevers, Den Haag.
Seidman, I., 2019. Interviewing as qualitative research: a guide for researchers in education and the social sciences, Fifth edition. ed. Teachers College Press, New York, NY.
Spitzner, L., 2002. Honeypots: tracking hackers. Addison-Wesley, Boston.
Steinmetz, K.F., 2015. Craft(y)ness: An Ethnographic Study of Hacking. British Journal of Criminology 55, 125–145. https://doi.org/10.1093/bjc/azu061
Švábenský, V., Čeleda, P., Vykopal, J., Brišáková, S., 2021. Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security 102, 102154. https://doi.org/10.1016/j.cose.2020.102154
Taylor, P.A., 1999. Hackers: crime in the digital sublime. Routledge, London ; New York.
van de Weijer, S.G.A., Holt, T.J., Leukfeldt, E.R., 2021. Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements. Computers in Human Behavior Reports 4, 100113. https://doi.org/10.1016/j.chbr.2021.100113
van 't Hoff-de Goede, M.S., van der Kleij, R., van de Weijer, S.G.A., Leukfeldt, E.R., 2019. Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. Research and Documentation Centre (WODC), The Hague.
Vetterl, A., 2020. Honeypots in the age of universal attacks and the Internet of Things (No. 944), Technical Reports. University of Cambridge.
Wall, D.S., 2001. Cybercrimes and the Internet, in: Wall, D.S. (Ed.), Crime and the Internet. Routledge, London, UK; New York, NY, pp. 1–17.
Weulen Kranenbarg, M., 2021. Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives, in: Weulen Kranenbarg, M., Leukfeldt, E.R. (Eds.), Cybercrime in Context, Crime and Justice in Digital Society. Springer International Publishing, Cham, pp. 195–216. https://doi.org/10.1007/978-3-030-60527-8_12
Weulen Kranenbarg, M., Ruiter, S., van Gelder, J.-L., 2021. Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. European Journal of Criminology 18, 386–406. https://doi.org/10.1177/1477370819849677
Yar, M., Steinmetz, K., F., 2019. Cybercrime and society, 3rd edition. ed. Sage Publications, Thousand Oaks, CA.

CRediT author statement

Asier Moneva: Conceptualization, Investigation, Writing - Original Draft, Writing - Review & Editing, Supervision, Project administration. **Rutger Leukfeldt**: Conceptualization, Investigation, Writing - Review & Editing. **Marco Romagna**: Investigation, Writing - Review & Editing.

Authors' bio

Asier Moneva is a postdoc at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and the Center of Expertise Cyber Security at The Hague University of Applied Sciences (THUAS). He is a criminologist interested in how, when, and where cybercrime occur, focusing on the human factors involved. He mainly relies on quantitative methods and data science to do research, and enjoys collaborating with researchers from other disciplines, practitioners, and professionals. With his research, Asier aims to generate knowledge to better understand cybercrime, and to find solutions to reduce it or mitigate its impact.

Rutger Leukfeldt is a senior researcher at the NSCR and director of the Centre of Expertise Cyber Security at THUAS. He has been doing research into the human factor of cybercrime for 15 years. During that period, he was involved in both fundamental academic research and applied research for companies and governments. Rutger carries out both quantitative and qualitative studies, but his expertise lies in qualitative methods. Over the years, he analyzed numerous large scale police investigation and interviewed both cybercriminals and victims.

Marco Romagna is a lecturer and researcher at the Centre of Expertise Cyber Security of THUAS. He has studied cybercrime both in its criminological and legal dimension, focusing on the human element. He mainly uses qualitative methods such as interviews and virtual ethnograpy. He is also a PhD candidate at Leiden University researching hacktivism and focusing on the motivations, modus operandi, and organizational aspects of hacktivists.