Computers in Human Behavior 155 (2024) 108180

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Criminal expertise and hacking efficiency

Asier Moneva [a,b,*], Stijn Ruiter [a,c], Daniël Meinsma [b]

[a] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), the Netherlands
[b] Center of Expertise Cyber Security, The Hague University of Applied Sciences, the Netherlands
[c] Department of Sociology, Utrecht University, the Netherlands

ARTICLE INFO

Handling editor: Matthieu Guitton

Original content: The Journey to Cybercrime (Original data)

Keywords:
Criminal decision-making
Cyber kill chain
Expertise paradigm
Hacking
Sequence analysis

ABSTRACT

Criminal expertise plays a crucial role in the choices offenders make when committing a crime, including their modus operandi. However, our knowledge about criminal decision making online remains limited. Drawing on insights from cyber security, we conceptualize the cybercrime commission process as the sequence of phases of the cyber kill chain that offenders go through. We assume that offenders who follow the sequence consecutively use the most efficient hacking method. Building upon the expertise paradigm, we hypothesize that participants with greater hacking experience and IT skills undertake more efficient hacks. To test this hypothesis, we analyzed data from 69 computer security and software engineering students who were invited to hack a vulnerable website in a computer lab equipped with monitoring software, which allowed to collect objective behavioral measures. Additionally, we collected individual measures regarding hacking expertise through an online questionnaire. After quantitatively measuring efficiency using sequence analysis, a regression model showed that the expertise paradigm may also apply to hackers. We discuss the implications of our novel research for the study of offender decision-making processes more broadly.

1. Introduction

The Expertise Paradigm in criminology describes how the development of domain-specific skills and knowledge is related to offending (Nee, Gelder, Otte, Vernham, & Meenaghan, 2019; Nee & Ward, 2015).[1] In psychology, expertise has been defined as the combination of "skills and knowledge an individual develops through learning and concerted practice in a particular domain" (Nee et al., 2019, p. 483). In this way—intentionally or not—individuals develop expertise along a continuum of competence that discriminates novices from masters (Chi, 1989; Chopin, Paquette, & Fortin, 2022; Nee & Ward, 2015). Nee and colleagues (2019) argue that the Expertise Paradigm complements the Rational Choice Perspective (Cornish & Clarke, 1986) and extends explanations for offending with automatic or unconscious decision making. Since early research on burglars (Wright, Logie, & Decker, 1995), studies have consistently shown that more criminal expertise results in greater situational awareness, which contributes to automate the crime-commission process (Nee & Ward, 2015). Therefore, the more expert burglars act more efficiently (Meenaghan, Nee, Vernham, & Otto, 2023; Nee & Meenaghan, 2006). Efficiency is essential to understanding the crime commission process, as it reveals how offenders optimize resources while minimizing risk and maximizing profits. Ultimately, this insight can serve to develop prevention measures aimed at rendering crime ineffective enough so as to discourage offenders from committing it.

However, ongoing discussions on whether cyber offenders differ from traditional offenders (Weulen Kranenbarg, Holt, & van Gelder, 2019; Weulen Kranenbarg, Ruiter, van Gelder, & Bernasco, 2018; Weulen Kranenbarg, Ruiter, & van Gelder, 2021), along with recent developments in criminal business models like cybercrime-*as*-a-service (Hyslip, 2020), raise questions about whether the observed relationship between criminal efficiency and expertise in offenders such as burglars (Meenaghan et al., 2023; e.g., Nee et al., 2019; Nee & Meenaghan, 2006), carjackers (Topalli, Jacques, & Wright, 2015), and online sex offenders (Chopin et al., 2022), holds true for hackers; that is, whether higher hacking expertise is also related to higher hacking efficiency. A better understanding of the relationship between expertise and efficiency in hacking could shed light on the modus operandi of cybercriminals and identify attack patterns of novices and experts. In this way it would be possible to identify different attack vectors leading to tailored

* Corresponding author. Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), the Netherlands.
E-mail address: amoneva@nscr.nl (A. Moneva).

[1] Expertise with criminal activity as an outcome has also been called *dysfunctional* expertise, as opposed to *functional* expertise (Nee & Ward, 2015).

https://doi.org/10.1016/j.chb.2024.108180
Received 5 December 2023; Received in revised form 13 February 2024; Accepted 16 February 2024
Available online 23 February 2024

responses, as well as addressing emerging threats before they escalate.

Hacking can be broadly defined as the unauthorized trespassing of a computer system (for a discussion, see Holt, 2020). A system can be, for example, a personal computer, a workstation, or a web server. There are multiple ways to hack into a system ranging from social engineering to the use of malware, and not all of them require the same skills (for reviews see Furnell, 2014; Maimon & Louderback, 2019).[2] Website defacements are hacks that modify the content of a web page without permission of its administrator (e.g., Holt, 2011; Moneva, Leukfeldt, van de Weijer, & Miró-Llinares, 2022), and are often carried out by script kiddies who want to gain status within the hacker community (Holt, 2007), or by hacktivists with political motives (Romagna, 2020). A common target of defacements are websites created with WordPress, the most popular open-source content management system for website creation. Not all hackers are equally efficient though. For example, a study found that financially motivated hackers can be either fast and unsophisticated, or slow and sophisticated (Wieren, Doerr, Jacobs, & Pieters, 2016). Another survey-based study reported that hackers with rational information processing tendencies used more effective hacking methods than those with experiential tendencies (Bachmann, 2010). These results suggest that hackers acting rationally would try to minimize their effort while navigating cyberspace toward their target.

This pre-registered study builds on existing research and extends it to the online environment. In particular, we examine the efficiency of IT students in hacking a website within a controlled online environment that, for 1 h, monitors their online behavior.

2. Criminal expertise and the hacking process

Decades ago, criminologists suggested that expert offenders are able to process environmental cues effortlessly and make better target selection choices (Brantingham & Brantingham, 1978). Unlike traditional offenders, hackers carry out crimes online. To navigate cyberspace, hackers must pass instructions to a computer by means of clicks and keystrokes. So, while physical distance is an offline impediment that hackers do not face online (e.g., Yar, 2005), they may encounter other obstacles, such as the natural or computer languages they must know to access certain information. Here, expertise is key, as it is more likely that hackers with more knowledge and IT skills will overcome these obstacles with less effort, adopting a more efficient modus operandi. In contrast, a lack of expertise can also lead hackers to retrace their steps or take additional steps, which requires more time and effort and is therefore less efficient. This means that contingent upon the level of expertise of hackers and their decision making, the crime commission process unfolds in different ways.

There are indeed multiple ways to hack into a system, each demanding a different expertise. Less technical hacks usually involve some form of social engineering, like phishing, or an oversight on the part of the system administrator. Against the myth, it is not always necessary to be an IT expert to hack a target. Cybercrime-*as*-a-service makes affordable toolkits, such as remote access tools or phishing kits, available to potential hackers (Hyslip, 2020). The tutorials that accompany these products make hacking easy for many. Within the more technical hacking methods, there are also degrees of sophistication (Maimon & Louderback, 2019). One of the least sophisticated methods is the brute-force attack, which consists of implementing an automatic method to test a massive list of passwords against a login system. A more efficient version of this hack would be a dictionary attack, which would only use the most popular passwords. But even this small refinement requires some expertise from the offender, who has to know where to find a directory of frequently used passwords. The next step on the sophistication ladder includes SQL injections, which insert malicious code to extract data from a vulnerable data-driven application. When the target of the hack is a website, a common technique is the directory or path traversal attack. This type of attack relies on the existence of standard directory structures in systems to access sensitive files, such as usernames or passwords. Systems based on directory templates, such as WordPress, are particularly vulnerable to this type of attack. Among those that require a higher degree of sophistication are hacks that employ malicious software to collect sensitive information through the keystrokes of their victims—spyware—or to take control of a system—trojan. This wide range of techniques, that includes just a few (for a review, see Furnell, 2014), shows that hacking is a cybercrime that admits different expertise, which makes it attractive to a wide group of cyber offenders.

Despite the variability of the crime commission process, criminologists and computer scientists have attempted to organize crime in a standardized sequential process using analytical frameworks such as crime scripts (Cornish, 1993), and the cyber kill chain (Hutchins, Cloppert, & Amin, 2011). For Hutchins et al. (2011), the cyber kill chain can be captured in a sequence of seven phases (Table 1). From the first phase of *reconnaisance* to the last phase of *command and control*, hackers must act on a series of decisions that transport them through the kill chain in one way or another. Both crime scripts and kill chains have the same purpose: to comprehend the crime commission process to identify disruption points. Beyond formalizing the original phases, there is no standardized method for representing crime scripts or kill chains. The progressive model of phases, spanning from before, during, to after the commission of the crime, along with the apparent clarity it provides,

Table 1
The seven phases of the cyber kill chain applied to website defacement.

Phase	Label	Description	Website defacement example
1	Reconnaissance	Doing research to identify and select targets.	Gathering information about a target website like software version, plugins installed, and potential vulnerabilities.
2	Weaponization	Attaching malware to an exploit on a deliverable.	Creating a malicious script to exploit the identified vulnerabilities via code injection or file manipulation and embedding it in a file.
3	Delivery	Transmitting the deliverable to the target.	Sending the manipulated file to the website through a compromised plugin or injecting it directly into its directory.
4	Exploitation	Triggering the malware of the deliverable.	Executing the script to access sensitive files, compromise login credentials, or initiate remote code execution.
5	Installation	Fixing the malware to maintain presence inside the target.	Establishing a persistent foothold on the compromised website by modifying critical files.
6	Command and control	Establishing a channel between the controller server and the target.	Setting up a channel to remotely control the website, often through a backdoor or hidden communication protocol.
7	Actions on objectives	Interacting with the target further.	Defacing the website by, for example, altering content or displaying political messages.

Source for "label" and "description": Hutchins et al. (2011).

[2] Note that cybercrime-*as*-a-service has democratized access to cybercrime, offering tools, processes, and services that require minimal knowledge and skills at a low cost (Hyslip, 2020). Notably, many of these materials are readily available on the clear web at no cost, introducing a new dimension to the crime commission process and making it particularly accessible to non-expert and potential hackers.

encourages presenting scripts in a linear manner. With few exceptions that explicitly acknowledge cyclic processes in the script (Matthijsse, van 't Hoff-de Goede, & Leukfeldt, 2023), most scripts are presented linearly (Holt & Lee, 2022; Hutchings & Holt, 2015; Loggen & Leukfeldt, 2022). The resulting linear schematic representations of crime, whether scripts or kill chains, may therefore be overly simplistic, and important nuances for understanding crime in cases that are not straightforward (e.g., incomplete attempts, recurrence in certain phases, return to previous phases) would get lost.

To delineate a more realistic crime-commission process, we apply sequence analysis—a method to study and interpret patterns in a series of events (Ritschard, 2021). We collect objective behavioral data to analyze quantitatively and in detail how IT students navigate the phases of the kill chain. The resulting sequences of actions reveal new patterns of behavior in the hacking process, while sequence indicators also serve to propose a novel quantitative measure of criminal efficiency.

3. The present study

Based on the Rational Choice Perspective (Cornish & Clarke, 1986), we assume that hackers are rational beings who will try to maximize rewards with minimum effort. In their attempt to trespass a computer system, hackers would then try to follow the most efficient methods: those that lead to a successful hack with the least effort. To measure the efficiency of a hack, it is first necessary to determine which way of hacking requires the least effort. In this study we assume that following the sequence of steps described in the cyber kill chain (Hutchins et al., 2011) is the most efficient method of performing a hack, as long as the sequence is followed in a linear fashion, without recourse in its steps. *Hacking efficiency* can therefore be defined as the extent to which a hacker successfully progresses through the phases of the kill chain while reducing phase repetition and sustaining forward momentum in the sequence. However, not all hackers are equally efficient. Although some follow the cyber kill chain sequentially, others act chaotically, jumping from phase to phase until they eventually might stumble upon a solution. To better understand the decision making process of offenders in cyberspace and the factors associated with it, we developed and pre-registered a novel research design to address the following research question:

What is the relationship between individual hacking expertise and hacking efficiency?

3.1. Hypotheses

The expertise paradigm (Nee et al., 2019) suggests that those individuals who have experience in performing a specific task will perform it more efficiently as they automate part of the process (e.g., Nee & Meenaghan, 2006). A study showing that higher IT skills may be positively related with the commission of the more technical offenses, such as hacking (Weulen Kranenbarg, Holt, & van Gelder, 2019), provides indirect evidence for this relationship. Individuals with more hacking experience and skills might better understand the structure of the website, its hosting, the software it uses, and what vulnerabilities it has as a result. It is possible that the most expert hackers already possess—or know where to find—the information needed to execute the hack, which would help them move up the kill chain. Experts would then navigate hacking-related websites and acquire the right information from them with more ease than novices due to greater awareness and expertise. This reasoning leads us to formulate the following two hypotheses:

H_1: IT students with hacking experience will conduct more efficient attempts to hack a target website.

H_2: IT students with more IT skills will conduct more efficient attempts to hack a target website.

3.2. Pre-registration

In line with open science practices, and to prevent HARKing (i.e., hypothesizing after the results are known) and p-hacking (i.e., manipulating analysis to achieve statistical significance), we pre-registered the present study. The study was pre-registered in the Open Science Framework (OSF) in April 2022, after the data were collected and the distribution of the variables was reported in a codebook, but before conducting the analyses presented in this manuscript. For details, see the pre-registration.

3.3. Ethical considerations

This research was reviewed by the Ethics Committee for Legal and Criminological Research (CERCO) in April 2021. After making some minor remarks regarding the content of the informed consent and the challenges of conducting research during COVID-19 times, the committee declared no ethical concerns.

4. Methods

Using the facilities of The Hague University of Applied Sciences, we prepared a computer lab to collect a range of objective and subjective measures from participants through their participation in a two-part study: a website defacement challenge,[3] and an online questionnaire about online behavior and IT knowledge.

4.1. Participants

For this study we intended to recruit a sample that resembled as closely as possible a sample of young hackers. A recent review of 23 studies on the characteristics of cybercriminals concludes that most are young, highly educated males (Edwards, Williams, Peersman, & Rashid, 2022). That is why we recruited participants from technical programs at The Hague University of Applied Sciences—students of IT security and computer engineering—through an advertisement distributed online by their teachers. Participants were incentivized with €10 for their participation in the form of an online store gift-card, raised to €20 if they hacked and defaced the target website. To participate in the study, participants had to sign an informed consent. We recruited 72 participants and, after excluding two participants (ID = QAKJ7y, V7DwJe) for failing to record their data correctly and one participant (ID = dDz2Dd) for speeding during the questionnaire (completed in 2.5 min), collected valid data from 69 in seven sessions split over two days in September 2021. Participants had a mean age of 21 years (SD = 2.8) and were mostly male (94.2%).

4.2. The computer lab

The lab is maintained by university staff and consists of two adjacent computer rooms with 26 and 28 computers respectively. About half of the computers were made available in an attempt to distribute participants evenly across the rooms. All computers had the same specification and ran on Windows 10. The computers were connected to the Internet and, using Oracle Virtual Machine VirtualBox version 6.1.18, incorporated two virtual machines (VMs) each on a host-only network. A system snapshot was preserved for both VMs, allowing the virtual environment to be manually restored to the initial state of the challenge at the end of each session. The first VM was an Ubuntu 20.04.2 Live Server (amd64) and had installed WordPress version 5.7.2, a popular open-source content management system. This VM was used to host the target website. The second VM was a default Kali Linux machine, a Debian-derived

[3] Such challenges are commonly known as *capture-the-flag* exercises in cyber security training (see Cowan, Arnold, Beattie, Wright, & Viega, 2003).

Linux distribution designed for digital forensics and penetration testing. To monitor participants and collect objective behavioral measures we installed the monitoring software Actual Keylogger on each computer.

4.3. Study design

In the first part of the exercise, participants were assigned to their own computer and took part in a 1-h monitored capture-the-flag exercise in which they were asked to deface the target WordPress website that was hosted in the first VM. One way to do this was, for example, to obtain the administrator's password by exploiting a vulnerability. As the website was created by one of the researchers and hosted in a controlled environment, this was a harmless task. The website was made vulnerable by.

- allowing all files in the WordPress folder to be read by any user;
- setting a very short administrator's password, which could be obtained by performing a dictionary attack—an efficient type of brute force attack—on the login page of the website;
- having an unencrypted backup of the administrator's password stored in the machines folder structure, which could be reached using the remote code execution vulnerability in the (installed) WordPress Plugin wpDiscuz 7.0.4.

Following the kill chain, we present in Table 2 three examples of intrusions that would exploit each of the vulnerabilities. Note that participants were not asked to erase their digital traces as part of the exercise, so such concealing behaviors we would expect from expert hackers are outside the scope of the study.

In the second part, an online questionnaire designed with LimeSurvey was administered to collect additional individual measures from participants. We assigned each participant a unique identifier, which allowed us to link the data they generated during both exercises.

Table 2
Three examples of the cyber kill chain exploiting the vulnerabilities in the target WordPress website.

Phase	Label	Sequence 1	Sequence 2	Sequence 3
1	Reconnaissance	Identifying that the website is built in WordPress and its file structure.	Finding the login page of the WordPress website and any potential users.	Identifying the version of wpDiscuz plugin in the WordPress website and its vulnerabilities.
2	Weaponization	Writing a malicious script that leverages the fact that no permissions are required to read the file.	Using a dictionary attack tool to guess the administrator password.	Crafting a payload to exploit the remote code execution vulnerability.
3	Delivery	Uploading the script to the website's WordPress directory.	Launching the dictionary attack on the login page.	Injecting the payload into the website.
4	Exploitation	Executing the script to read sensitive files, like the one containing the password.	Gaining unauthorized access to the WordPress admin panel.	Executing the payload to retrieve the unencrypted backup with the administrator's password.
5	Installation	Modifying the theme file to ensure persistence, and embedding the script.		
6	Command and control	Establishing a hidden communication channel between the compromised website and the attacker's server via a backdoor.		
7	Actions on objectives	Defacing the website, and using the website to launch further attacks like spreading malware or stealing user data.		

4.4. Data

The monitoring software allowed us to accurately capture the activity of the participants during the capture-the-flag exercise (Fig. 1), including the keystrokes introduced and their source. Keystrokes included keyboard keys and mouse buttons. Keyboard keys can produce character strings like "words", and special keys like 'control' (< Ctrl >), 'enter' (< Enter >), or 'backspace' (< BkSp >). The source of the keystrokes indicates where they were entered, usually an application, a URL or an IP. It is therefore possible to precisely reconstruct the text generated by the participants with the keyboards in a given context, such as a search query in a web browser or an instruction in a network mapping application, even if the participants made a typing mistake that they later corrected. A limitation of the monitoring software is that it does not collect keystrokes introduced in the Kali Linux VM, so we had to manually collect all commands introduced in the Kali Linux command prompt using the 'history' command. The commands were then saved as a. txt file. After processing and cleaning the data, we identified 2881 unique keystrokes, 1073 (37.2%) of which were commands from the Kali Linux command prompt.

With the online questionnaire we collected participants' sociodemographic information, online routine activities, self-reported cyber-offending and victimization experiences, objective IT skills, and asked whether participants sought external help to complete the task. We also collected data on the time participants took to complete the questionnaire. The data analyzed contain observations from 69 participants across 23 variables.

4.5. Measures

In theory, the most direct measure of hacking efficiency would be the time it takes for a participant to deface the website. However, within the time constraints of the capture-the-flag exercise, only one of the participants succeeded (*ID* = uzSQ9H). So, instead, we looked at the sequence of actions they took to hack the website using the cyber kill chain as a reference. The main outcome variable is therefore the hacking efficiency shown by participants *while* performing the capture-the-flag challenge as captured by the monitoring software. The two main predictors are the objective IT-skills of participants and their hacking experience. These two measures were collected using the online questionnaire based on that of Weulen Kranenbarg, Ruiter, & van Gelder, 2021.

4.5.1. A hacking efficiency index

Since only one participant hacked the website, we cannot compare successful participants and then calculate who was fastest to determine their efficiency. We can, however, examine the sequence of steps they took and how far they got according to the cyber kill chain, defined as "a systematic process to target and engage an adversary [in this case a website] to create desired effects" (Hutchins et al., 2011, p. 4). To identify how far the participants got in the kill chain, we asked two IT security experts to annotate each keystroke according to one of the phases of the kill chain or indicate 'unclear' if they were not sure. The experts, who were technical security instructors at the same institution where the participants were studying, taught courses on topics like cyber operations—focusing on the fundamentals of pentesting and SOC analysis—and were therefore well aware of the capabilities of the participants. Because of this knowledge, the experts were in an advantageous position to understand the participants' hacking process. To facilitate the annotation task, we provided the experts with a graphical user interface created with Visual Basic for Applications in a Microsoft Excel macro-enabled spreadsheet along with detailed instructions on how to

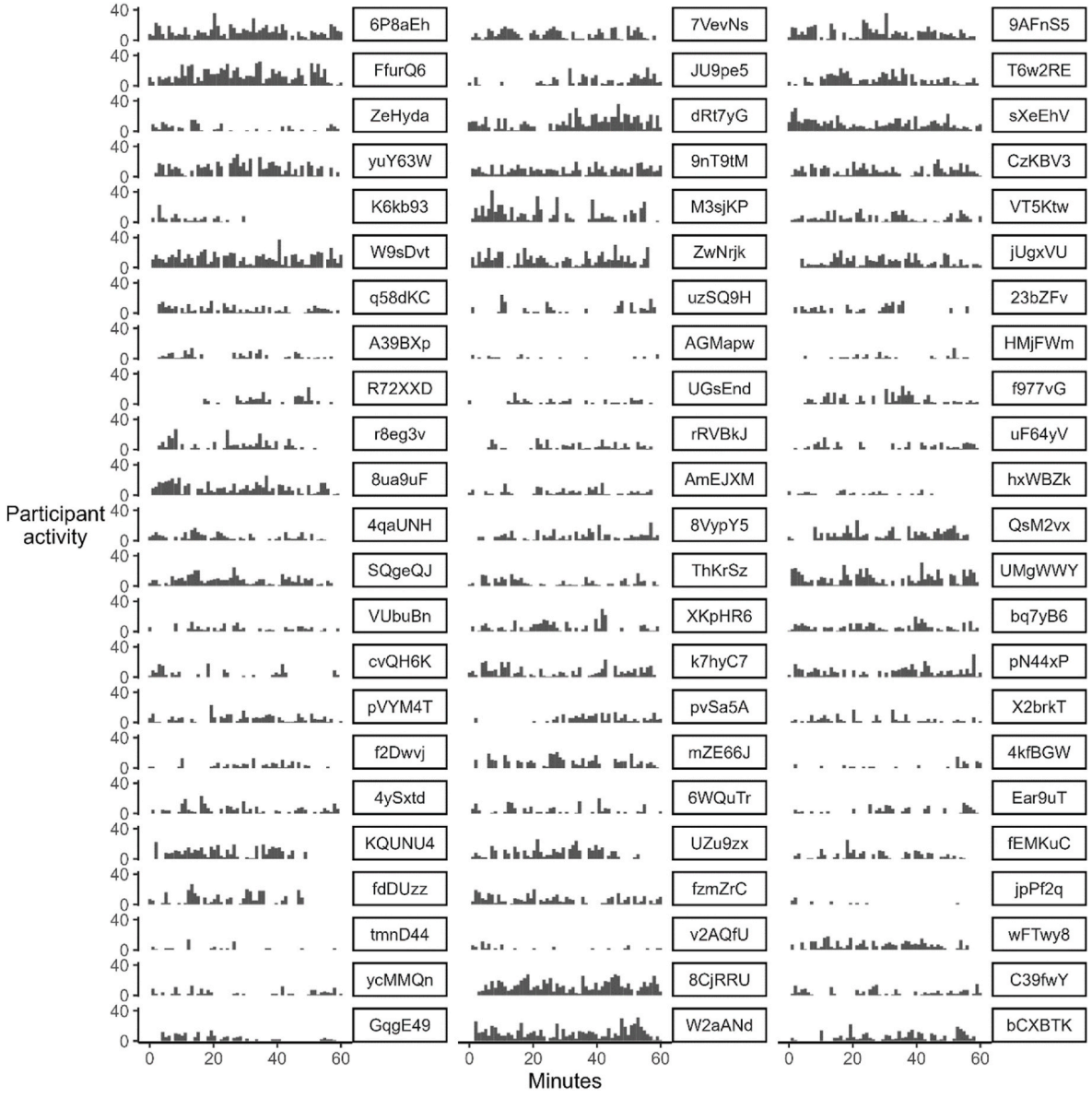

Fig. 1. Participants' activity during the 1-h exercise.

carry out the task. Such instructions included the definition of each of the phases of the kill chain, a description of the keystroke data, and a user manual for the interface.

We then assessed the degree of agreement between the two experts with the inter-rater reliability score produced by Krippendorff's alpha (Krippendorff, 1970). The alpha showed little to no agreement between the raters ($\alpha = 0.067$). As we anticipated a large amount of uncertainty on the part of the experts, we pre-registered a rule to favor certainty over uncertainty. In the event that one of the two experts was unable to classify the commands or keystrokes according to one of the categories of the kill chain (i.e., indicated "Unclear"), the opinion of the expert who classified them prevailed. Disagreements between the two experts were then resolved by a third expert, who was the head of their research group.

This process revealed 146 sequences distributed among 69 participants (Fig. 2). Note that each time participants opened a new instance of the Kali Linux command prompt to execute commands we had to record their keystrokes as an independent sequence because the command line keystrokes are not time-stamped and therefore cannot be joined to the rest of the keystrokes in a timeline. For this reason, 48 (69.6%) participants produced more than one sequence—up to a maximum of 6 ($M = 1.9$; $SD = 1.1$).

Based on the sequences, we claim that the hacking efficiency of the participants should be considered higher in relation to the kill chain when they:

- reach more phases;
- repeat fewer phases, and/or
- go forward more often than backwards.

These conditions can be measured using sequence analysis. We used the TraMineR R package (Gabadinho, Ritschard, Müller, & Studer, 2011) to calculate three indicators per sequence and participant. The first indicator was the *proportion of visited states* (Brzinsky-Fay, 2007), a numeric value normalized to range from 0 to 1 that measures how far participants got in the kill chain. The second was an inverted version of the *recurrence index* (Pelletier, Bignami-Van Assche, & Simard-Gendron, 2020), a numeric value normalized to range from 0 to 1 that measures how often participants took a step backwards in the kill chain. The third was the *degradation index* (Ritschard, 2021), a numeric value normalized

Fig. 2. Participants' hacking sequences according to the phases of the cyber kill chain.

to range from 0 to 1 that measures phase transitions in the right direction. Since the order of the phases does not matter to calculate the proportion of visited states, but it does matter to calculate the recurrence and degradation indicators, we calculated the first by aggregating all sequences per participant, while we calculated the other two on each individual sequence and then averaged them per participant.

We then explored whether combining these factors into a single efficiency construct would yield meaningful results. To do so, we simulated sequences, conducted bivariate analyses, and theorized several scenarios (Appendix A). The analyses revealed that there is a statistically significant and negative relationship between inverted recurrence and sequence length that disappears when accounting for sequence length. This suggests that these efficiency indicators should not be combined into one unless controlling for sequence length. So, we decided to deviate from the pre-registration and add *sequence length* (i.e., the sum of the length of all sequences produced by each participant) to our control variables, and combine all efficiency indicators into a single outcome variable. Therefore, the *hacking efficiency index* is a normalized average value of the three efficiency indicators, ranging between 0 and 1, where higher values represent higher efficiency. TraMineR uses Optimal

Matching (Abbott & Forrest, 1986) to work with sequences of different lengths.

To demonstrate the performance of the index, Fig. 3 scores the efficiency of six synthetic sequences of different lengths that represent extreme theoretical scenarios. The *best scenario* represents a sequence of seven phases corresponding to those of the kill chain. This sequence has the maximum proportion of visited states, the minimum recurrence, and the minimum degradation. It obtains, therefore, a normalized efficiency score of 1. In contrast, the worst scenario represents a sequence whose properties result in an efficiency of 0. Fig. 3 then shows three sequences representing the least efficient scenarios with respect to each of the three efficiency indicators: a sequence with the minimum proportion of visited states (*lowest normalized proportion of visited states* = 0); a sequence with maximum recurrence (*lowest normalized inverted recurrence* = 0), and a sequence with the maximum degradation (*lowest normalized degradation* = 0). Finally, it displays a sequence that combines 7 phases randomly sampled from our data. In these examples, the maximum recurrence scenario also happens to be the least efficient.

Fig. 4 shows the distribution of the three efficiency indicators, and the hacking efficiency index using the participants' sequence data.

4.5.2. Objective IT-skills

We use the IT-skills test developed by Weulen Kranenbarg, Ruiter, & van Gelder, 2021 to measure the objective IT skills of participants. The test is based on other online tests and was adapted with the assistance of the Team High Tech Crime of the Netherlands Police. It consists of 10 items with 5 response options each, including "I don't know". To prevent participants from searching for answers on the Internet, we added a timer of 45 s to each question. Correct answers scored 1 point, while incorrect ones subtracted 0.25. Answering with "I don't know" or not answering, neither added nor subtracted. Scores could therefore range from −2.5 to 10 points. Fig. 5 shows the distribution of the participants' scores.

4.5.3. Self-reported hacking experience

We used the same questions as Weulen Kranenbarg, Holt, & van Gelder, 2019 to collect a series of self-reported hacking measures from participants. They were asked how often in the past 12 months they had engaged in the following five hacking behaviors without permission.

- breaking into or logging in to a network, computer or web account by guessing the password;
- gaining access in another way to a network, a computer, a web account or files stored on it;
- taking over a network, computer or web account;
- changing the content of a website or an online profile; and
- deleting, adding, damaging or modifying someone else's computer files.

The question was presented as a matrix, and to facilitate understanding the behaviors, each type of hacking was presented as a brief description of a behavior with examples rather than a name or formal definition. For example, we asked *"How often in the past twelve months did you 'break into or* log *in to a network, computer or web account by guessing the password' without permission?"* Response options ranged from "0 times" to "5 or more", with the additional option of "I don't know". Due to the right-skewed distribution of the variable, we also decided to dichotomize it between 0 times (no experience) and at least one time (experience). Fig. 6 shows the variable distribution in its continuous and dichotomous version, and indicates that one quarter of the participants had at least some hacking experience.

4.5.4. Control variables

As control variables, we included an integer numerical measure of the age of the participants, a dichotomous measure of whether the area of their highest completed education is *informatics and IT*, or any other area as a reference category, and an integer numerical measure of the length of the sequences produced by the participants (Fig. 7). A recent quasi-experiment using virtual environments suggests that older burglars conduct more efficient searches than younger burglars (Meenaghan et al., 2023). In the context of this study, it is possible that older participant have had more time to develop their IT skills, have more hacking experience and, therefore, are more efficient. The same rationale applies to those participants who have studied informatics and IT. In Appendix A we showed that the relationship between the efficiency indicators and the efficiency index varies as a function of sequence length—to the point of changing direction. Therefore, we deviated from the pre-registration and controlled for sequence length. In the preregistration, we also considered controlling whether participants sought outside help during the capture-the-flag exercise, but decided not to do so because we considered it endogenous to efficiency and in order to keep the model as parsimonious as possible.

4.6. Analytic strategy

In the preregistration we indicated that we would perform a confirmatory factor analysis to test whether the three indicators of hacking efficiency belonged to the same latent construct and, if not, we would model each indicator separately. Finally, we decided not to perform this analysis and to fit an ordinary least squares (OLS) regression model to a single outcome variable for the sake of interpretability. Thus, we examined the relationship between the predictors (i.e., IT skills, and hacking experience) and the outcome (i.e., hacking efficiency), while

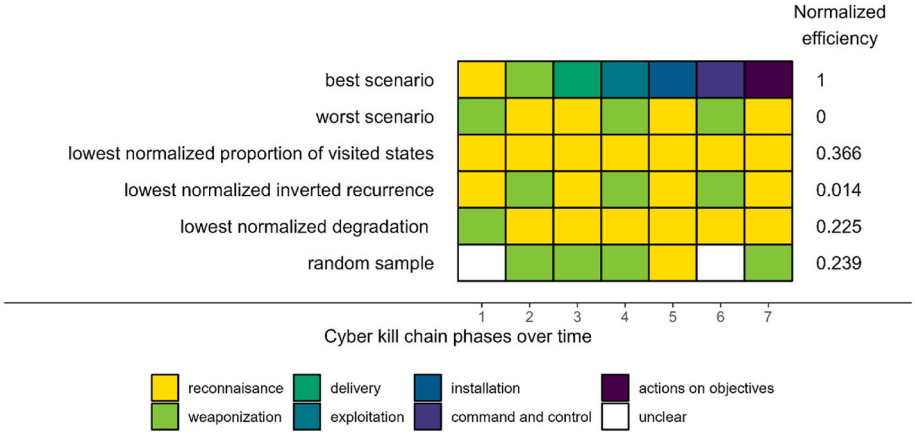

Fig. 3. Example synthetic sequences with efficiency scores.

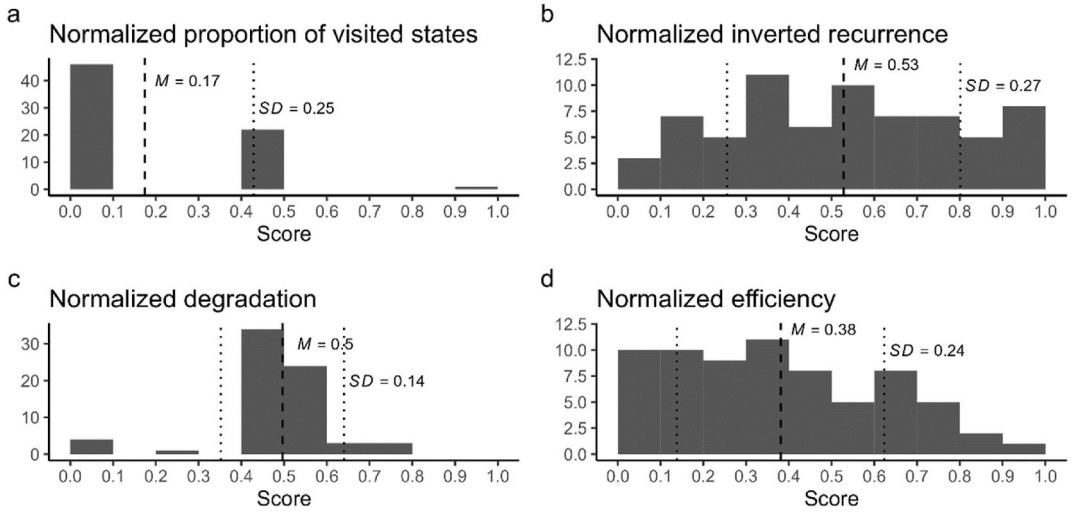

Fig. 4. Distribution of participants' hacking efficiency indices (a, b, c), and hacking efficiency (d).

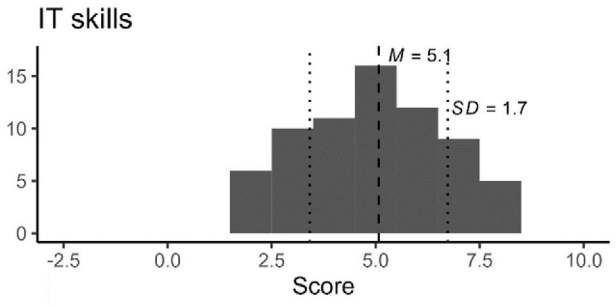

Fig. 5. Distribution of participants' IT-skills scores.

controlling for the age of participants, their IT background, and sequence length. We standardized all variables in the model to have a mean of zero and a standard deviation of one in order to compare the impact of the predictors on the outcome. Appendix B presents the model diagnostics.

Given that we pose directional hypotheses, we use one-tailed statistical significance tests with the standard threshold in the social sciences ($\alpha = 0.05$). If we observe a positive and statistically significant relationship between hacking experience and the outcome after controlling for the other covariates, we will interpret this as support for H_1; if we observe a positive and statistically significant relationship between IT skills and the outcome after controlling for the other covariates, we will interpret this as support for H_2. If we find positive associations that are not statistically significant, we will not interpret these as support for the hypotheses but we will discuss the influence of sample size on the results. In any other case, we will reject the hypotheses. Because we use a cross-sectional research design, causal inferences are not warranted, so any support for the hypotheses will be interpreted with caution.

5. Results

The model results are shown in Table 3. Model 1 uses the dichotomous version of hacking experience (as pre-registered), while Model 2 uses its continuous version. Regarding H_1, the results of both models show that more IT skills are statistically significantly related to higher hacking efficiency. Holding all other variables constant, a one standard deviation increase in IT skills corresponds to a 0.44 standard deviation increase in efficiency in Model 1, and to a 0.4 in Model 2. Regarding H_2, more hacking experience is not statistically significantly related to higher efficiency in either model. Considering the distance to the significance threshold, this may be due to a lack of statistical power. Within our sample, a one standard deviation increase in hacking experience corresponds to a 0.19 standard deviation increase in efficiency in Model 1, and to a 0.1 in Model 2. As for the control variables, longer sequence length is statistically significantly related to less efficiency in Model 1 but not in Model 2. A one standard deviation increase in sequence length corresponds to about a −0.19 standard deviation decrease in efficiency in both models. Effect sizes for IT skills, hacking experience, and sequence length can be considered medium, small, and small respectively (Cohen, 1988). The remaining control variables appear to be unrelated to efficiency.

The coefficients of determination (Adjusted R-squared) indicate that these expertise models would explain between 13% and 15% of the variance in hacking efficiency.

6. Discussion

This pre-registered study tested whether the expertise paradigm (Nee et al., 2019) applied to cybercrime commission. For that purpose, we recruited a sample of IT security students to participate in an hour-long monitored challenge to deface a website made vulnerable by design. At the end of the exercise, we collected additional individual measures

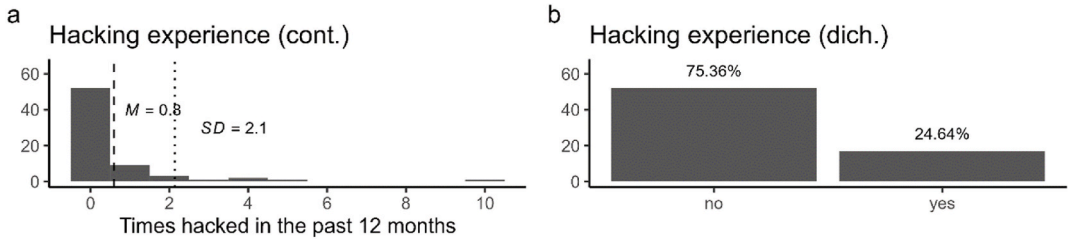

Fig. 6. Distribution of participants' cyber offending and hacking experience.

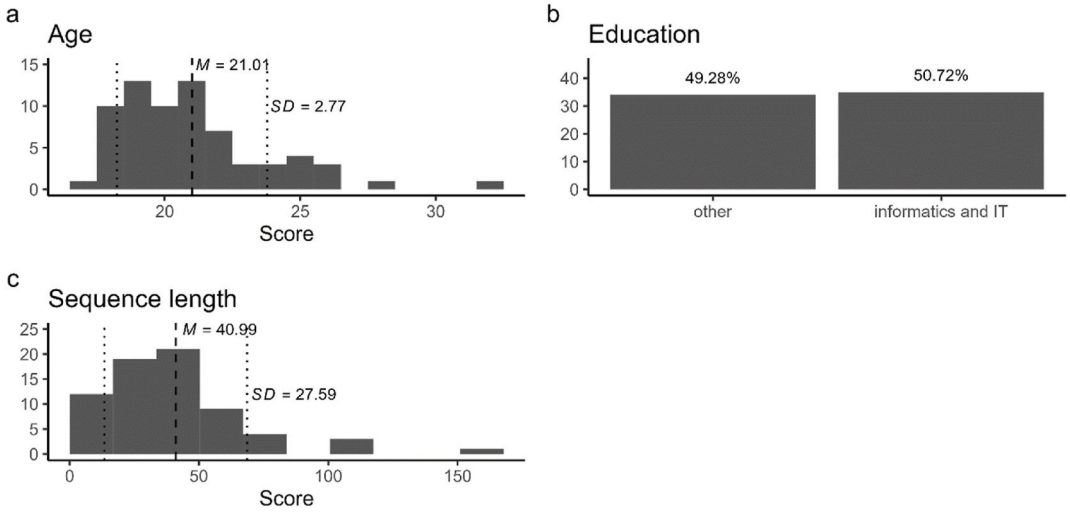

Fig. 7. Distribution of participants' age (a), education (b), and sequence length (c).

Table 3
OLS models results.

Variable	Model 1 (dich. hacking experience)			Model 2 (cont. hacking experience)		
	Std. β	[95% CI]	One-tailed p-value	Std. β	[95% CI]	One-tailed p-value
(Intercept)	0.000	[-0.222, 0.222]	0.500	0.000	[-0.225, 0.225]	0.500
IT skills	0.437	[0.196, 0.678]	0.000	0.400	[0.162, 0.638]	0.001
Hacking experience	0.186	[-0.05, 0.421]	0.060	0.104	[-0.129, 0.336]	0.189
Age	−0.012	[-0.243, 0.219]	0.460	0.007	[-0.225, 0.239]	0.476
IT education	−0.111	[-0.349, 0.127]	0.178	−0.096	[-0.336, 0.145]	0.215
Sequence length	−0.193	[-0.422, 0.037]	0.049	−0.186	[-0.419, 0.047]	0.058
R-squared	0.214			0.193		
Adjusted R-squared	0.151			0.129		

from the participants with an online questionnaire. We then examined the relationship between individual hacking experience, measured as the combination of hacking experience and IT skills, and hacking efficiency, measured as the sequence of phases of the kill chain followed by the participants. The findings suggest that the expertise paradigm may hold for potential hackers. In such case, rational choice perspectives aiming to explain cybercrime (e.g., Newman & Clarke, 2003) should take criminal expertise into account.

Regarding H_1, we found that participants with more objective IT skills showed higher hacking efficiency. From an expertise paradigm, these domain-specific skills could provide potential hackers with a superior ability to recognize environmental cues that are useful during the exercise (Nee & Ward, 2015). This result is consistent with the findings of Weulen Kranenbarg, Holt, & van Gelder, 2019, who suggest that there is a positive relationship between IT skills and cybercrime offending. Regarding H_2, however, we did not find a significant association between having hacking experience and hacking efficiency. Note that this result may be due to a lack of statistical power.[4] As for the other factors examined, we found that older participants did not show greater hacking efficiency, which contrasts with the finding that older burglars performed more efficient searches inside houses (Meenaghan et al., 2023). It is possible that we did not observe any differences because most participants were relatively young. We also found that participants whose last completed education was in informatics and IT did not show greater hacking efficiency. Another study found that having an IT background was not significantly related to cyber offending either (Weulen Kranenbarg, Ruiter, van Gelder, & Bernasco, 2018). This suggests that IT skills are also developed outside the educational context, in which case peers may have an influence. Finally, in the pre-registered model we found that those participants who made more attempts to hack the website, measured as more kill chain phases covered, were significantly less efficient.

The study is novel from both a theoretical and methodological perspective. First, it links a psychological paradigm used in criminology, the expertise paradigm (Nee & Ward, 2015), to a cybersecurity framework, the cyber kill chain (Hutchins et al., 2011), to advance the understanding of cybercriminal decision making. Second, the study proposes a new methodological approach to measure hacking efficiency. It uses sequence analysis (Ritschard, 2021)—a type of quantitative analysis with many applications in social sciences but seldom used in criminology—to measure actual efficiency and not simply self-reported metrics. Both innovations take advantage of the interdisciplinary nature of criminology.

6.1. Theoretical contribution

Following the broader trend of extending social science paradigms to explain cybercrime, this study extends the application of the expertise paradigm to cyberspace. We conceptualized hacking efficiency as the sequence of phases of the cyber kill chain followed during the hacking process (Hutchins et al., 2011), and measure it quantitatively using sequence analysis (Ritschard, 2021). Here we measure a specific type of hack in which both motivation and target location are fixed. In this hack, the primary motivation is to commit the crime, but due to the relative inexperience of the participants, there is a secondary motivation that is preparatory. Since the target was fixed in the vulnerable website,

[4] For a significance level of $\alpha = 0.05$ and a desired power of 0.80, the sample size required to detect small ($f^2 = 0.02$), medium ($f^2 = 015$), and large ($f^2 = 0.35$) effect sizes using a generalized linear model (Cohen, 1988), would be 647, 92, and 43, respectively.

participants could only decide how to carry out the hack. If the participants had been given complete freedom, as in the case of criminal hackers, we might have observed different modus operandi. It is also important to note that most criminological research focuses on completed crimes and thus overlooks why some attempts might fail, which could be useful for crime prevention. This research analyzed data from 69 hacking attempts of IT students, and found them to be highly chaotic, meaning that a disorganized modus operandi may contribute to criminal failure.

Criminologists pioneered the study of crime as sequences of decisions and actions, developing frameworks such as crime scripts (Cornish, 1993). More recently, cybersecurity developed attack models known as kill chains (e.g., Hutchins et al., 2011), which serve as the cyber equivalent of crime scripts. Both frameworks have in common that they deconstruct the offending process into phases, which contributes to both understand its intricacies and identify key disruption points. Here we frame kill chains as a hacking process, in which efficiency varies depending on how offenders progress along the chain. In this study, we argued that progressing linearly along the chain would be the most efficient way to hack, but we could not provide direct evidence for this. However, by monitoring participants in real time as they attempted to hack a website, we did uncover complex sequences of decisions based on their behavior that we associated with indicators of hacking efficiency. Quantitatively analyzing these sequences revealed differences based on the proportion of phases they visit, the phases they repeat, and the extent to which they progress along the sequence. This could be the initial step to define a typology of hackers based on their hacking efficiency (e.g., efficient, reversed, persistent, careful, chaotic, lucky, stuck, inefficient; see Appendix A).

Our findings suggest that the hacking process does not follow the cyber kill chain linearly, but may actually be more chaotic. Attackers may navigate back and forth within the kill chain, trying various techniques and looking for new targets until they make tangible progress. When attempting to convey simplified offending processes using linear models like the cyber kill chain, we misrepresent the crime commission process for offenders who do not follow a linear pattern of behavior, unintentionally perpetuating biased or unrealistic portrayals of crime. Actually observing behavior with methods such as video, virtual reality, or monitoring software—rather than presenting a simplified, scripted model of crime—can help determine how structured offenders actually behave. For example, a study conducted in a virtual environment found that inexperienced burglars exhibit chaotic search patterns inside the house (Nee et al., 2019). The chaotic nature of cyber offending is also acknowledged by the unified kill chain: “advanced attacks can be regarded as phased progressions, but individual attack phases may be bypassed, occur more than once or occur out of sequence” (Pols, 2023, p. 14). We found that inexperienced hackers go back and forth during the hack, repeating phases of the kill chain, retracing their steps, and even skipping some phases that are supposed to be sequential. Such non-linear crime commission processes would have implications for situational crime prevention (Clarke, 1980). On the one hand, there may be recurring steps in which the measures can multiply their effect; on the other, there may be steps that do not occur in the expected sequence or are outright omitted. This would render the effect of the measures limited or null. It is therefore important not only to identify the crime steps, but also to weight their importance within the sequence in scripts and chains.

6.2. Limitations

This study implemented a novel method for monitoring of cybercriminal behavior in real time. The combination of capture-the-flag exercises and monitoring software allows to collect objective measures of online behavior, which are more accurate than self-reported measures (Parry et al., 2021), and thus overcome some of the previous research limitations. In doing so, however, we encountered unique challenges. One of the challenges was recruiting participants for the study, as the capture-the-flag task was time consuming and required a hard to find hacking skill set. We intended to recruit 100 participants, but in the end we got valid responses from 69, which can be considered a small sample size. Another challenge was to classify the behavior of the participants into kill chain phases. For this purpose, we recruited IT security experts and provided them with instructions and a semi-automated tool for the classification task. The task proved arduous, as it was sometimes possible to classify the same behavior into different categories of the kill chain. For example, hitting the ‘a’ key can mean different things. It could be an option to ‘use’ or ‘list all’ in a tool, or it could be input to a web application. In addition, many of the keystrokes recorded lacked context, were not correctly spelled, or were halfway through. This is comparable to the challenges of natural language processing, where a word may have a different meaning depending on the part of speech it is in, where words have to be corrected without knowing the intent of the writer, or where incomplete words may result in different words when completed. Anticipating a low degree of agreement among the experts, we pre-registered a criterion to favor certainty over uncertainty when classifying keystrokes, and called on a third expert to resolve disagreements. Overall, the task posed a challenge to the experts that may have a direct impact on the results. Future research should consider developing more detailed coding schemes and providing training to experts.

Other limitations were inherent to the keylogger we used. Firstly, the keylogger we used did not record the keystrokes that were entered into the second VM because it was running the Kali Linux operating system. This was an oversight in the piloting phase of the study. To mitigate this limitation, we had to manually collect the commands entered into the command line of this VM. These keystrokes were ordered sequentially, but did not have a time stamp, which prevented us from being able to merge them with the rest of the keystrokes. We opted to create distinct sequences for these commands instead. This solution had no impact on measures such as proportion of visited states or sequence length, but likely affected others such as recurrence and degradation. Although command line keystrokes are arguably the most relevant, it is important to note that in the second VM we did not log keystrokes entered in other applications. As a result, the analyzed sequences were incomplete. Secondly, we operationalized each stage of the kill chain by analyzing sets of keystrokes originating from the same program, as identified by the keylogger. Typically, these sets of keystrokes conclude with a mouse click or the enter key, indicating an instruction to the computer. We considered this criterion to be appropriate for this study. However, it is possible to interpret several instructions as part of the same phase, potentially grouping several phases together. Alternatively, a temporal criterion could be employed to operationalize a phase (i.e., the set of actions performed every 30 s). In such cases, it could be challenging to classify multiple actions into a single phase, as they may correspond to several phases simultaneously. The challenge for the researchers lies in defining the unit of analysis in sequences of actions, such as the crime commission process.

Finally, our model is limited in accounting for predictors of hacking such as self-control and peer influence, commonly found in the criminological literature (e.g., Holt, Bossler, & May 2012). The effect of self-control may be especially relevant in criminal hackers, while peer influence plays an important role in hacking communities. It is possible that self-control influences factors such as concentration and patience, which would in turn affect decision making. For example, hackers with lower self-control may follow the kill chain more chaotically than those with high self-control. On the other hand, we considered including a peer influence variable that measures the solicitation of external help during the hacking exercise, but we discarded the possibility after reasoning that it was endogenous to efficiency, since it would be part of resource management. Aside from possible parsimony problems, it is possible that these variables would have increased the explanatory power of our hacking expertise model.

6.3. Future research directions

Since this is the first study of its kind, we anticipate many future lines of research. Regarding theory, it is crucial to investigate the applicability of paradigms such as Expertise, which were originally conceived for traditional criminals, in the context of cybercriminals. Current research is uncovering similarities and differences between these two types of offenders (Weulen Kranenbarg, Ruiter, van Gelder, & Bernasco, 2018, Weulen Kranenbarg, Holt, & van Gelder, 2019, Weulen Kranenbarg, Ruiter, & van Gelder, 2021), which could be crucial in determining whether current criminological theories can explain cybercrime or whether new ones are needed. Regarding methods, it would be interesting to explore the possibility of combining kill chains (Hutchins et al., 2011) with crime journeys (Bernasco, 2014) and crime scripts (Cornish, 1993) to obtain an integrated analytic framework useful for social sciences and computer sciences. This would make findings comparable across disciplines. In addition, it would be useful to develop a process, either automated (e.g., machine learning) or manual (e.g., coding scheme) to improve the classification of online behaviors into kill chain phases. Regarding research design, other types of capture-the-flag exercises would allow the study of other cybercrime types in which, for example, the type of crime is different, or the target is not fixed in advance. In addition, having participants perform a hacking task until they succeed or give up would allow to examine the crime-comission process without the time pressure imposed by our research design. Studies in computer labs are ideal for testing experimental conditions related to criminological theory such as the Rational Choice Perspective (Clarke & Cornish, 1985), since they would allow manipulation of conditions such as the effort made during the crime or the rewards obtained at the end. Regarding samples, more expert hackers, whether criminal or ethical, should be recruited to increase the internal validity of the findings. Larger samples would increase the statistical power, which in turn would increase the reliability of the findings. In sum, this study has the potential to spearhead a field of research that could achieve several breakthroughs.

More broadly, our findings show that the process of crime commission may not be as linear as previously thought, but rather quite disorderly. This invites the wider criminological audience to assess whether sequence analysis (Ritschard, 2021) can contribute to the advancement of the discipline by showing how crime actually unfolds.

CRediT authorship contribution statement

Asier Moneva: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Project administration, Methodology, Investigation, Formal analysis, Data curation. **Stijn Ruiter:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Daniël Meinsma:** Writing – review & editing, Resources, Investigation.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used ChatGPT 3.5 in order to improve language and readability. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Declaration of Competing interest

All authors declare no conflict of interest.

Data availability

I have shared the link to my data/code at the Attach File step.
The Journey to Cybercrime (Original data) (OSF)

Acknowledgements

This publication is part of the project “How do cyber offenders commit crime online? Tracking the digital footprint of hackers” (with project number “VI.Veni.221R.024”) of the research programme “NWO Talent Programme” which is (partly) financed by the Dutch Research Council (NWO).

Appendix A. Simulated sequence scenarios

In this section we examine in depth how the hacking indicators combine to produce the hacking efficiency index. To do so, below we simulate data, analyze it and examine different theoretical scenarios.

Since we suspected that sequence length might change the way the indicators relate to each other, which would directly affect the interpretability of the index, we simulated all possible combinations of kill chain phases for all sequences of up to seven phases ($7 + 7^2 + 7^3 + 7^4 + 7^5 + 7^6 + 7^7 = 960{,}799$) and drew a random sample of 1050 observations with replacement, clustered by sequence length, to experiment with. The combination of the three indicators, based on their highest and lowest possible values, can result in eight possible theoretical scenarios of efficiency. For reference, we named each scenario in Table 4 and ranked them according to how many efficiency conditions they meet.

Table 4
Theoretical scenarios resulting from the combination of the three efficiency indicators

Scenario	Normalized proportion of visited states	Normalized inverted recurrence	Normalized degradation	Label	Efficiency conditions met
1	high	high	high	efficient	3
2	high	high	low	reversed	2
3	high	low	high	persistent	2
4	low	high	high	careful	2
5	high	low	low	chaotic	1
6	low	high	low	lucky	1
7	low	low	high	stuck	1
8	low	low	low	inefficient	0

Fig. 8 shows the pairwise correlation and plot matrix between the three efficiency indicators, the efficiency index, and the sequence length. The diagonal shows the distribution of each variable using a kernel density estimator. We note a significant negative correlation between normalized proportion of visited states and normalized inverted recurrence ($r = -0.347$; $p \leq 0.001$), suggesting the three efficiency indicators should not be

combined into a single construct. This relationship disappears when removing sequences shorter than three phases ($r = -0.009$; $p = 0.814$), and even flips when removing sequences with no recurrence ($r = 0.538$; $p \leq 0.001$) or sequences shorter than four phases ($r = 0.212$; $p \leq 0.001$). Note that any of these three conditions is present in 64.1% of the sample analyzed. We also found a positive and significant correlation between sequence length and normalized efficiency suggesting that we should adjust for sequence length to account for efficiency.

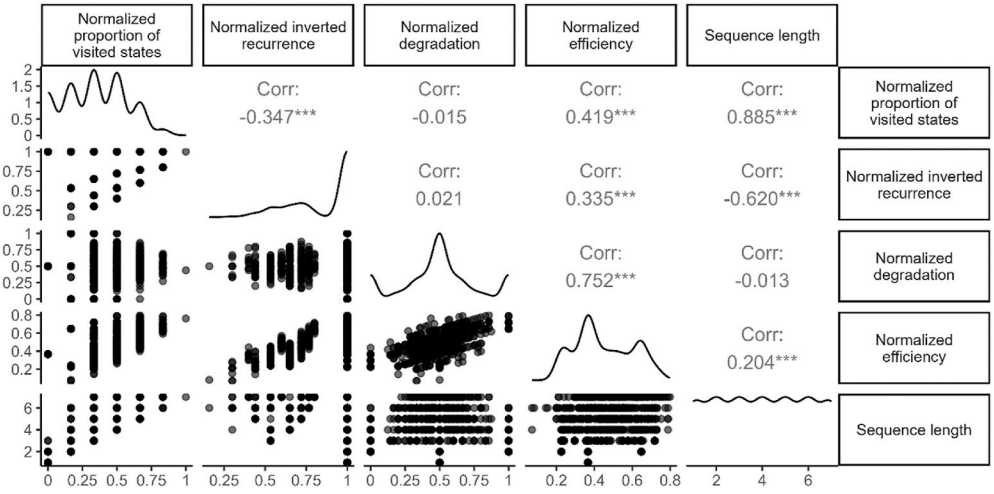

Fig. 8. Theoretical relationship between the three efficiency indicators, sequence length, and efficiency.

We then proceeded with the full set of sequences to explore the correspondence between the efficiency of the simulated observations and the theoretical scenarios. We operationalized the high and low conditions of each indicator using a quantitative criterion. We considered indicators with values ≥ 0.5 as high and indicators with values < 0.5 as low. For example, *reversed* scenarios should have a normalized proportion of visited states value ≥ 0.5, a normalized reversed recurrence value ≥ 0.5, and a normalized degradation value < 0.5. This strategy allowed us to assign each observation to a theoretical scenario and examine the distribution. Table 5 shows the distribution of all possible scenarios along with the efficiency index. Because of how the indicators covary (Fig. 8), it turns out that not all theoretical scenarios are possible. The *persistent* and *chaotic* scenarios are impossible. In line with our conceptualization, we observed that more theoretically efficient scenarios are also associated with a higher efficiency index.

Table 5
Distribution and mean efficiency of the six possible theoretical scenarios

		Distribution		Normalized efficiency			
Scenario	Condition	n	%	Min.	Mean	SD	Max.
efficient	Visitp≥0.5; Recu≥0.5; Degrad≥0.5	277,124	28.843	0.479	0.596	0.088	1.000
reversed	Visitp≥0.5; Recu≥0.5; Degrad <0.5	231,916	24.138	0.320	0.524	0.081	0.780
careful	Visitp <0.5; Recu≥0.5; Degrad≥0.5	184,884	19.243	0.239	0.462	0.087	0.789
lucky	Visitp <0.5; Recu≥0.5; Degrad <0.5	129,157	13.443	0.201	0.375	0.067	0.561
stuck	Visitp <0.5; Recu <0.5; Degrad≥0.5	86,844	9.039	0.014	0.305	0.063	0.451
inefficient	Visitp <0.5; Recu <0.5; Degrad <0.5	50,874	5.295	0.000	0.243	0.061	0.324

Appendix B. Model diagnostics and robustness checks

Fig. 9 shows the model diagnostics of the two OLS models for—from left to right—linearity, normality, and influential values. The somewhat horizontal red line in the "Residual vs Fitted" plots shows that the relationship between the predicted values and the residuals may be linear. This suggests that a generalized linear model like OLS may therefore be a good approach to model such a relationship. The distribution of observations along the dashed line in the "Normal Q-Q" plots shows good alignment between the distribution of theoretical quantiles and standardized residuals, suggesting that the models meet the assumption of normality. The dashed lines in the "Residuals vs Leverage" plot show the threshold to determine if there are any outliers that may influence the model results. In the first model, observations 10, 26, and 68 may be considered outliers but not influential, whereas in the second model three observations, 10, 26, and 60 may be considered outliers but again not influential.

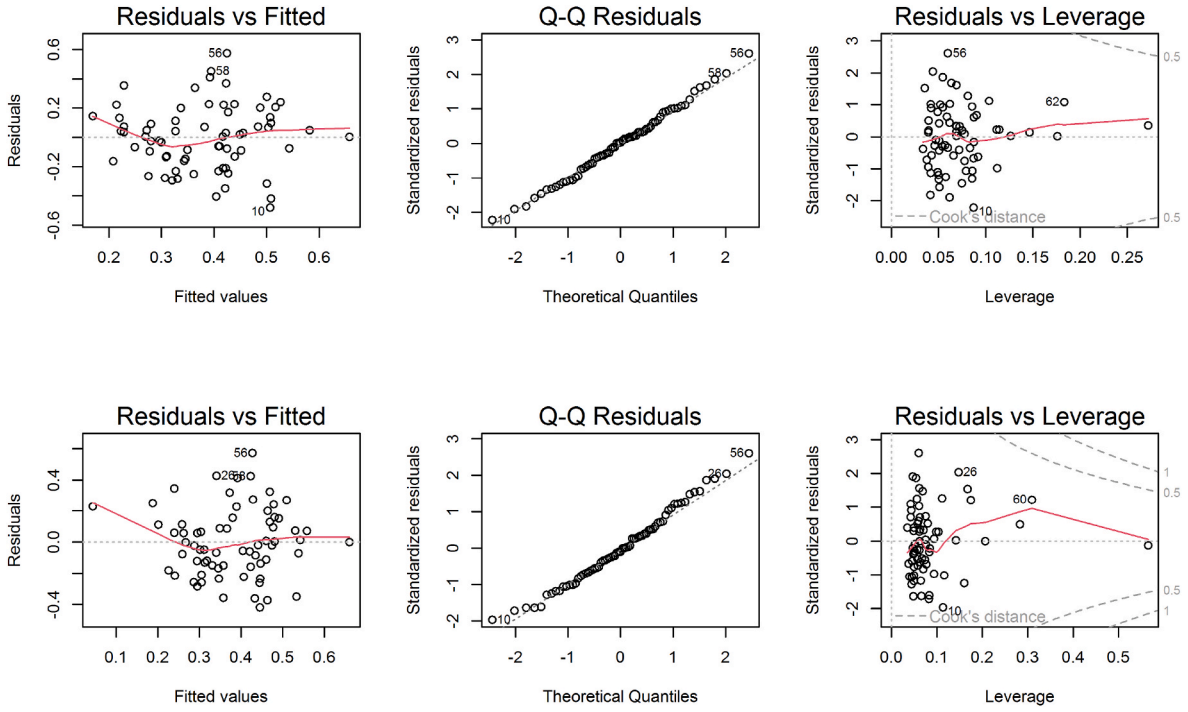

Fig. 9. Diagnostics of linearity, normality, and influential values for the OLS models (model 1 above; model 2 below).

In addition to assessing whether the observations in our sample can be considered influential with Cook's distance, we computed DFBETAS. DFBETAS serve to quantify change in the regression estimates when each observation is individually excluded from the analysis. When the change is greater than a threshold determined by $2/\sqrt{n}$, the excluded observation can be considered influential (Belsley, Kuh, & Welsch, 1980). Fig. 10 shows the DFBETAS that exceed this threshold, which correspond to 16 observations.

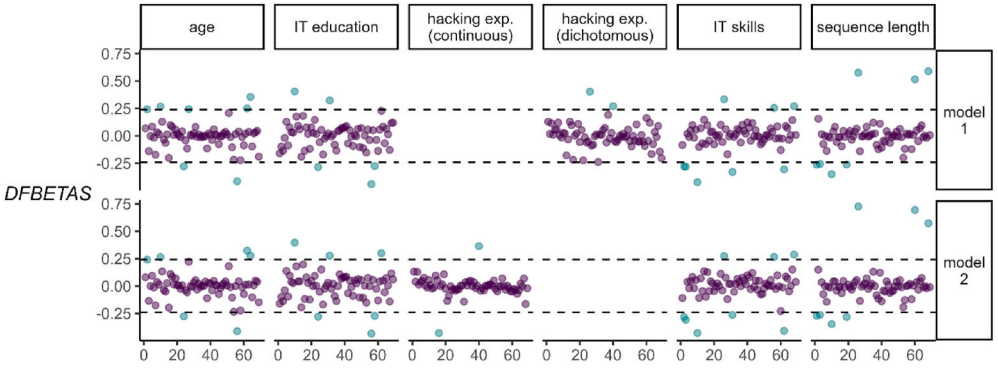

Fig. 10. DFBETAS and thresholds for influential values.

To determine the impact of these influential values on the model estimates, we performed an additional robustness check. Fig. 11 shows the estimates of the full models, as well as those of the 16 models in which we remove one of the influential observations at a time. As can be seen, the observations considered influential by the DFBETAS are in fact not so, as the variance of the standardized betas and their 95% CI is minimal in all cases. These results suggest that the results presented in models 1 and 2 are robust.

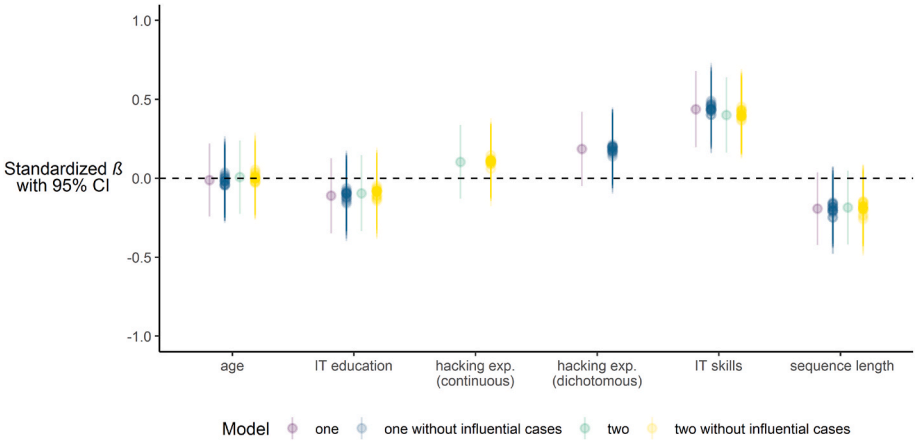

Fig. 11. Model estimates with and without influential observations.

References

Abbott, A., & Forrest, J. (1986). Optimal matching methods for historical sequences. *Journal of Interdisciplinary History, 16*(3), 471. https://doi.org/10.2307/204500

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1&2), Article 643656.

Belsley, D. A., Kuh, E., & Welsch, R. E. (1980). *Regression diagnostics: Identifying influential data and sources of Collinearity* (1st ed.). Wiley. https://doi.org/10.1002/0471725153

Bernasco, W. (2014). *Crime journeys: Patterns of offender Mobility (Oxford Handbooks Editorial board*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199935383.013.49

Brantingham, P. J., & Brantingham, P. L. (1978). In M. D. Krohn, & R. L. Akers (Eds.), *A theoretical model of crime site selection* (p. 105118). Beverly Hills, Calif.: Sage Publ.

Brzinsky-Fay, C. (2007). Lost in transition? Labour Market Entry sequences of School Leavers in Europe. *European Sociological Review, 23*(4), 409–422. https://doi.org/10.1093/esr/jcm011

Chi, M. T. H. (1989). In L. B. Resnick (Ed.), *Learning from examples via self-explanations*. Routledge. https://doi.org/10.4324/9781315044408-8.

Chopin, J., Paquette, S., & Fortin, F. (2022). Geeks and Newbies: Investigating the criminal expertise of online sex offenders. *Deviant Behavior, 1–17*. https://doi.org/10.1080/01639625.2022.2059417

Clarke, R. V. (1980). "Situational" crime prevention: Theory and practice. *British Journal of Criminology, 20*(2), Article 136147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice: A Review of Research, 6*, Article 147185.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale: N.J: L. Erlbaum Associates.

Cornish, D. B. (1993). *Crimes as scripts. 3045*. Coral Gables, FL: US Department of Justice.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York: Springer-Verlag.

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). *DARPA information survivability conference and exposition* (Vols. 120–129). Washington, DC, USA: IEEE Comput. Soc. https://doi.org/10.1109/DISCEX.2003.1194878

Edwards, M., Williams, E., Peersman, C., & Rashid, A. (2022). *Characterising cybercriminals: A review*. Retrieved from http://arxiv.org/abs/2202.07419.

Furnell, S. (2014). *Hackers, viruses and malicious software*. Routledge. https://doi.org/10.4324/9781843929338.ch9

Gabadinho, A., Ritschard, G., Müller, N. S., & Studer, M. (2011). Analyzing and Visualizing state sequences in R with TraMineR. *Journal of Statistical Software, 40*(4). https://doi.org/10.18637/jss.v040.i04

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171–198. https://doi.org/10.1080/01639620601131065

Holt, T. J. (2011). In T. Saadawi, & L. Jordan, Jr. (Eds.), *The attack dynamics of political and religiously motivated hackers*. Carlisle, PA: Strategic Studies Institute.

Holt, T. J. (2020). In T. J. Holt, & A. M. Bossler (Eds.), *Computer hacking and the hacker Subculture*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_31.

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

Holt, T. J., & Lee, J. R. (2022). A crime script analysis of Counterfeit identity Document Procurement online. *Deviant Behavior, 43*(3), 285–302. https://doi.org/10.1080/01639625.2020.1825915

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online Stolen data Market. *British Journal of Criminology, 55*(3), Article 596614. https://doi.org/10.1093/bjc/azu106

Hutchins, E., Cloppert, M., & Amin, R. (2011). In L. Armistead (Ed.), *6th international conference on information warfare and security*. Washington, DC: Academic Publishing International Limited. March.

Hyslip, T. S. (2020). In T. J. Holt, & A. M. Bossler (Eds.), *Cybercrime-as-a-Service operations*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_36.

Krippendorff, K. (1970). Estimating the reliability, systematic Error and random Error of Interval data. *Educational and Psychological Measurement, 30*(1), 61–70. https://doi.org/10.1177/001316447003000105

Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in The Netherlands. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09448-z

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(1), Article 191216. https://doi.org/10.1146/annurev-criminol-032317-092057

Matthijsse, S. R., van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z

Meenaghan, A., Nee, C., Vernham, Z., & Otto, M. (2023). A comparison of younger and older burglars undertaking virtual burglaries: The development of skill and automaticity. *Journal of Experimental Criminology*. https://doi.org/10.1007/s11292-023-09573-x

Moneva, A., Leukfeldt, E. R., van de Weijer, S. G. A., & Miró-Llinares, F. (2022). 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

Nee, C., Gelder, J.-L., Otte, M., Vernham, Z., & Meenaghan, A. (2019). Learning on the job: Studying expertise in residential burglaries using virtual environments. *Criminology, 57*(3), 481–511. https://doi.org/10.1111/1745-9125.12210

Nee, C., & Meenaghan, A. (2006). Expert decision making in burglars. *British Journal of Criminology, 46*(5), 935–949. https://doi.org/10.1093/bjc/azl013

Nee, C., & Ward, T. (2015). Review of expertise and its general implications for correctional psychology and criminology. *Aggression and Violent Behavior, 20*, 1–9. https://doi.org/10.1016/j.avb.2014.12.002

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan.

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. *Nature Human Behaviour, 5*(11), 1535–1547. https://doi.org/10.1038/s41562-021-01117-5

Pelletier, D., Bignami-Van Assche, S., & Simard-Gendron, A. (2020). Measuring Life course Complexity with Dynamic sequence analysis. *Social Indicators Research, 152*(3), 1127–1151. https://doi.org/10.1007/s11205-020-02464-y

Pols, P. (2023). *The unified kill chain. Raising resilience against advanced cyber attacks*. Retrieved from https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf.

Ritschard, G. (2021). *Measuring the nature of individual sequences*. Sociological Methods & Research, Article 004912412110361. https://doi.org/10.1177/00491241211036156

Romagna, M. (2020). In T. J. Holt, & A. M. Bossler (Eds.), *Hacktivism: Conceptualization, techniques, and Historical View*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_34-1.

Topalli, V., Jacques, S., & Wright, R. (2015). "It takes skills to take a car": Perceptual and procedural expertise in carjacking. *Aggression and Violent Behavior, 20*, 19–25. https://doi.org/10.1016/j.avb.2014.12.001

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J.-L. (2019). Offending and victimization in the digital age: Comparing Correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending Overlap. *Deviant Behavior, 40*(1), 4055. https://doi.org/10.1080/01639625.2017.1411030

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*(3), 386–406. https://doi.org/10.1177/1477370819849677

Weulen Kranenbarg, M., Ruiter, S., van Gelder, J.-L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the Life-Course: An empirical comparison. *Journal of Developmental and Life-Course Criminology, 4*(3), 343–364. https://doi.org/10.1007/s40865-018-0087-8

Wieren, M. van, Doerr, C., Jacobs, V., & Pieters, W. (2016). In G. Livraga, V. Torra, A. Aldini, F. Martinelli, & N. Suri (Eds.), *Understanding Bifurcation of slow versus fast cyber-Attackers*. Cham: Springer International Publishing. Retrieved from http://link.springer.com/10.1007/978-3-319-47072-6_2.

Wright, R., Logie, R. H., & Decker, S. H. (1995). Criminal expertise and offender decision making: An experimental study of the target selection process in residential burglary. *Journal of Research in Crime and Delinquency, 32*(1), 39–53. https://doi.org/10.1177/0022427895032001002

Yar, M. (2005). The novelty of 'cybercrime': An Assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), Article 407427. https://doi.org/10.1177/147737080556056