Cybercrime Warfare Against People: Pessimistic Side of Online

João Sebe[1]
[1] Lusófona University of Porto, Portugal
joaosebe@gmail.com

Abstract. Cybercrime has become as common as the Internet itself and consequently, it is considered one of the biggest threats to unaware individuals who might become victims. Cyberattacks have already caused considerable damage to a huge number of companies and small businesses but not less important, to people. This paper aims to further advance discussions on cyberthreats, cognitive vulnerabilities and cyberpsychology through a critical reflection on the social and psychological aspects related to cybercrime. It also sights on the analyses of the psychological effects an attack might have on a victim, examine the motivation of criminals that perpetuate such attacks and the factors and vulnerabilities they exploit to become successful at it while educating about how these attacks can be prevented through prevention, detection, and investigation since they are not expected to fade from society anytime soon.

Keywords: Cybersecurity, cybercrime, cyberattacks, social impacts, psychological impacts, motivation, cybercriminals' profiling

1 Introduction

Over the last few decades, the Internet has transformed the world we live in. From changing businesses, education, government, healthcare to even changing the way we interact with our loved ones – it has become one of the key drivers to social evolution since everyone is somewhat dependent on computer networks and information technology solutions.

Although the Internet removed many communication barriers that previously existed and keeps us connected to the world almost instantaneously, along with its phenomenal growth, it became a place where numerous unfortunate events take place and where bad intended people practice criminal activity.

To better understand the relationship between technology and crime, it is important to establish the understanding of cybercrime and its effect on today's society. Cybercrime is a term that covers a broad scope of criminal activities by means of a computer and a network. Cybercrime is referred to the act of committing a criminal act using cyberspace as the communication medium [1]. Computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few [2].

Cyberattacks are described as events that attempt to compromise a system's integrity, confidentiality, or availability (technical or sociotechnical). These attacks can range from hacking and denial-of-service (DoS) attacks to ransomware and spyware

infections, and they can affect anybody from the public to a country's national infrastructure system [3].

Why cyberattacks flourish? Cyberattacks become more attractive and potentially more disastrous as our dependence on information technology increases. Cyberattacks are cheaper, convenient, and less risky than physical attacks [4]. Aside from a computer and Internet connection, cybercriminals only require a few expenses. They are not bound by distance, and they are tough to perceive and prosecute due to the anonymous nature of the Internet. Because cyberattacks against information technology are highly attractive, it is expected that the number, diversity, and sophistication of cyberattacks will continue to rise throughout the years [5].

2 Main threats

In the past years, we have seen a substantial increase in cyber criminality in the form of high-profile ransomware campaigns. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud. Cybercriminal's tactics are changing as businesses are being targeted rather than individuals, and while phishing attacks on individuals are on the rise, fewer are falling victim as people have become more aware [6].

2.1 Social engineering

Social engineering is a form of cybercrime that involves the use of deceit or trickery to persuade individuals into performing some unauthorized, unlawful, or illegal action. It seeks to exploit and take advantage of human psychology and is arguably the most effective way of committing a crime against an individual [15]. Phishing attacks are perhaps the most well-known, in which unsuspecting users are encouraged to click on a faulty link, enabling hackers to install malware and consequently gain access to the system. In all circumstances, social engineering assaults combine social interactions with technology exploitation, making it challenging for cybersecurity specialists in businesses and government organizations to build effective countermeasures [29].

2.2 Data breaches

Data breaches occur when sensitive, protected, or confidential information is copied transmitted, viewed, stolen, or utilized by an unauthorized individual to do so. According to the Identity Theft Resource Center, a recognized non-profit organization established to support victims of identity crime, released its United States of America data breach findings for the third quarter of 2021. For this period of time, the number of data compromise victims (160 million) is higher than the first and second quarter of 2021 combined (121 million) [7].

Not only data breaches, but unprotected cloud databases are to blame for the significant increase in victims. In addition, year-to-date (YTD), the overall number of

cyberattack-related data compromises is up 27% from 2020. Phishing and ransomware remain, by far, the most common threat vectors [7].

2.3 Internet of things

With the growing number of devices connected to the Internet, it is highly likely that we will see more attackers using the Internet of Things (IoT) to commit crimes. Many internet-connected devices sold to consumers lack basic cybersecurity provisions. With countless unsecured devices, vulnerabilities will continue to be exploited and used for activities (such as DDoS attacks) without the user's knowledge [6].

2.4 Cloud security

These days, small, medium, and large businesses are gradually adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend poses a huge challenge for cybersecurity, as traffic bypasses traditional points of inspection [8]. Only 40% of all data stored in the cloud is access secured, although most companies report they are concerned about encryption and security of data in the cloud [6]. This increased use of cloud technology to store sensitive information will continue to tempt cyberattackers.

2.5 Crypto jacking

Cryptocurrency has been gaining increased popularity over the last years and with its interest still strong, it opened an opportunity for cybercriminals to exploit. Crypto jacking - where an individual's computer processing power is used to mine cryptocurrency without the user's consent - will likely become a regular source of revenue for criminals [7]. Popular websites are expected to continue to be compromised, offering crypto mining malware to users, and software that, when executed in a web page, mines digital currency using the visitor's spare computer processing power [6].

3 The impact of cyberattacks

According to research, people are more inclined to react to the consequences of a cyberattack than to the attack itself [9] [10]. One example is a cyberattack in which malware infects a national power plant, knocking out power to hundreds of thousands of people. Individuals will be more concerned about the effect of the attack, i.e., being without power, thus having no warmth or ability to prepare food [11].

There are two key areas of impact studies aim to consider and provide an overview about based on the current research and thinking. These are the social and psychological (emotional and behavioral) impacts. The social impact of a cyberattack includes aspects such as the social disruption it causes in people's daily lives, as well as more widespread issues like anxiety or a lack of confidence in technology. Psychological

impact can include more personal aspects such as an individual's anxiety, worry, anger, outrage, depression and so on [11].

3.1 Emotional reactions to cybercrime

The psychological impacts of cyberattacks may even resemble those of traditional terrorism, depending on who the attackers and victims are [12]. Victims of cybercrime and internet attacks may experience emotional stress, which can lead to depression. There is also some evidence of Acute Stress Disorder (ASD) symptoms in victims of online attacks, such as anecdotal tales of intrusive memories, emotional numbing, and upset from virtual sexual assault victims [13].

The emotional impact of identity theft, for example, might cause a victim to become agitated and leave them feeling violated, deceived, vulnerable, angry, and powerless [14]. Victimization frequently causes outrage, worry, a desire for protection over liberty, and a lack of interest in embracing new technology due to a loss of trust in cyberspace. The sufferer may go through stages of grief, anger, or rage. Victims may even blame themselves and develop a sense of guilt in some circumstances; sextortion is a great example of this because of how it begins [15].

3.2 Learned helplessness

According to the findings, only about one-tenth of people (9%) feel "very" safe online. In addition, only half of the respondents polled (51%) said they would change their internet behavior if they were a victim [16]. These findings show that, people might accept a certain situation, even if it feels unpleasant just because they cannot understand the reasoning and the process behind it. Following this point, one might argue that persons may accept cyberattacks because of a sense of 'learned helplessness' [11].

Users may simply accept the risk of being victims due to a sense of learned helplessness and a lack of understanding about online attacks and how to settle an incident. Indirectly, the key question becomes whether people accept the reality of repercussions while hoping for a low severity.

Nowadays, where the average user is required to make many security-related decisions, putting him under pressure and sometimes causing anxiety. These behaviors include:

- not opening emails from a sender they do not recognize;
- not accessing unknown attachments;
- only downloading and running programs from trustworthy sources;
- the use of anti-virus software and security software (e.g., firewall);
- creating regular backups.

Due to a lack of awareness about the potential consequences of making poor selections, some of these options can generate anxiety in the user. Even when individuals are aware of the online threats, they may not always understand them. Due to the public's lack of awareness of cyberthreats and security measures, there may be a lack of public engagement with security issues and a general loss of trust in technology.

This also has been seen in the domain of information privacy in the context of new forms of technology, where some users now consider privacy as 'the boring bit' [17].

3.3 Cyberattack related variables

A variety of cyber-specific elements, such as the attacker's identity, the target's identity, the magnitude of the assault, as well as government awareness of a cyberattack and the timing of disclosure of a harmful event, influence the public reaction to a cyberattack [11].

Terrorists, hacktivists, and criminals are the three main types of actors, all of whom are capable of initiating assaults that may be considered severe public concerns [18]. Criminals are less likely to expose their true identify (assuming any identity, pseudonym or otherwise) in public since anonymity allows them to operate more freely [11]. Furthermore, the identity of the target might influence public reaction.

4 Hacker's profiling and motivations

With scientists, practitioners, the public, and even hackers themselves debating what constitutes "hacking", who qualifies as a hacker, and their motivations for committing such crimes, hacking has become a contested topic. The definition of hacking as well as its meaning, have evolved over time, influencing how hackers are portrayed [19].

Hacking is the attempt, whether successful or unsuccessful, of exploiting computer and network vulnerabilities and consequently, to obtain unauthorized usage or access to a computer system [20].

4.1 Black Hat Hackers, White Hat Hackers and Grey Hat Hackers

Originally, the term "hacker" was used to describe exceptional and radical programmers in the field of computer science, gifted with "innovation, style and technical virtuosity" [20].

A clear difference is made within the computer security community between black hat hackers who exploit computer systems to cause harm or profit for themselves and white hat hackers who exploit computer systems to proactively uncover vulnerabilities that may be patched. Black hat trolls would typically be using forms of engagement that are not prescribed by the designer of the system and white hat trolls would be looking for ways to disable forms of non-prescribed engagement through research and education [21].

On the other hand, grey hat hackers operate in non-prescribed ways but are driven by a sense of public good rather than a desire to harm or earn personal advantage. They may see their acts as a method to show attack surfaces and put pressure on gatekeepers to improve their systems, or as a sort of "hacktivism" that exploits a system's weaknesses to advance a higher-order purpose of campaigning for human rights or "human security" [21].

Penetration testing, security research, and vulnerability disclosure may all be done by white hat and grey hat hackers. They might also take action by identifying negative actors, their motivations, and their tactics [21].

Furthermore, white hat and grey hat hackers may actively "troll back" or "troll the trolls", the black hat hackers, to counteract negative behavior.

4.2 Quantifying hacker motivations

Internal and external perpetrators have different motives and methods for accessing company data. External perpetrators or hackers are more skilled, organized, and innovative. Therefore, the data breach type depends on the perpetrator, their intentions, and the source of the threat [22]. The source is important because outsider activities will be more dangerous than those from the inside [23].

Due to the difficulty to reach out to hackers, to better understand their motivations, the following section relies on studies previously conducted. Although most literature that reports upon hackers' motivations merely explains which motivations can be deduced from the behaviors and interviews with hackers, these studies managed to shed some light on the differential importance attributed to motivations to hack and what vulnerabilities are being exploited to do so.

Thycotic Software Ltd (2018)

At Black Hat Conference, August 4-9, 2018, Thycotic Software Ltd conducted a survey of hackers to get their perspectives on vulnerabilities and attack vectors they find easiest to exploit.

With nearly 70% of 300+ poll respondents identifying as "White Hat Hackers," the study reveals a sizable proportion of participants committed to helping companies and organizations stay safe by exposing their most reliable exploits for IT systems. However, 30% of hacker participants anonymously acknowledged to possibly breaching the law in their hacking activities. Only 5% of those polled classified themselves as pure "Black Hat Hackers," who seek to breach networks for malevolent or personal gain [24].

The survey results were quite interesting, revealing some hacker's preferences when it comes to most attacked operating systems, the fastest means to get access to privileged accounts and the risky behaviors they exploited most often to access networks.

Despite Microsoft's efforts to increase cybersecurity, half of hackers said they were able to easily compromise both Windows 10 and Windows 8 in the year of 2017. Operating systems are only as safe as the people who use them and the configurations they have applied. Knowing that user account breach is almost certain, businesses should adopt a "zero-trust" policy that emphasizes least privilege to prevent over privileged accounts that offer hackers unrestricted access [24].

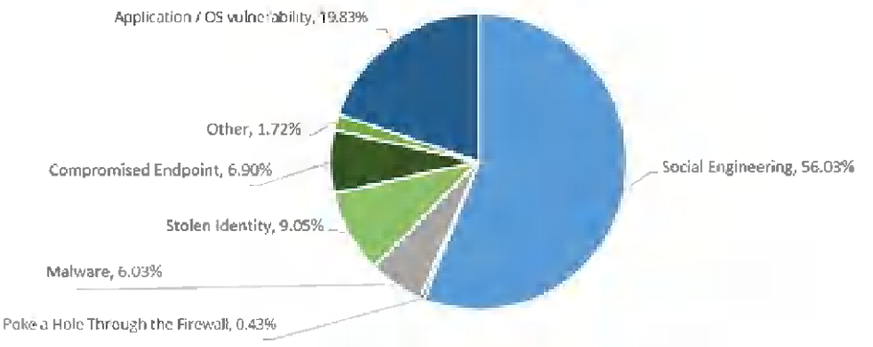

Fig. 1. Thycotic Black Hat 2018 Hacker Survey Report - "Which OS did you conquer the most in the past 12 months?" [24]

Once an attacker gains network access they can learn more about what software is being used, what patches are being deployed, when vulnerability scans are run, which systems and accounts have privileged access and how they can avoid detection. Vulnerabilities in applications and operating systems continue to be a major issue, with nearly 20% of hackers attacking unpatched systems. Identity theft is used by 10% of hackers to get network access, whereas malware and stolen endpoints are used by fewer than 7% [24].

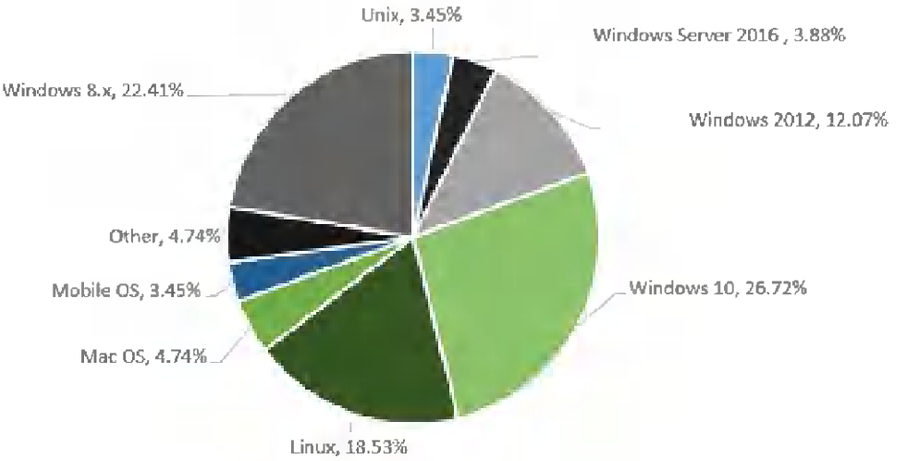

Fig. 2. Thycotic Black Hat 2018 Hacker Survey Report - "What's the fastest way for you to get onto a network to access privileged accounts?" [24]

Thycotic asked hackers to reveal an organization's most serious behavior-based security vulnerabilities — the ones they use the most to gain access to networks. Hackers revealed that half of their attacks discovered employees reusing passwords that had previously been compromised in past data breaches, allowing hackers easy access to the network. These findings demonstrate that employees suffer with poor password hygiene on a regular basis. Once hijacked, these end user accounts give hackers with an easy way to escalate privileges [24].

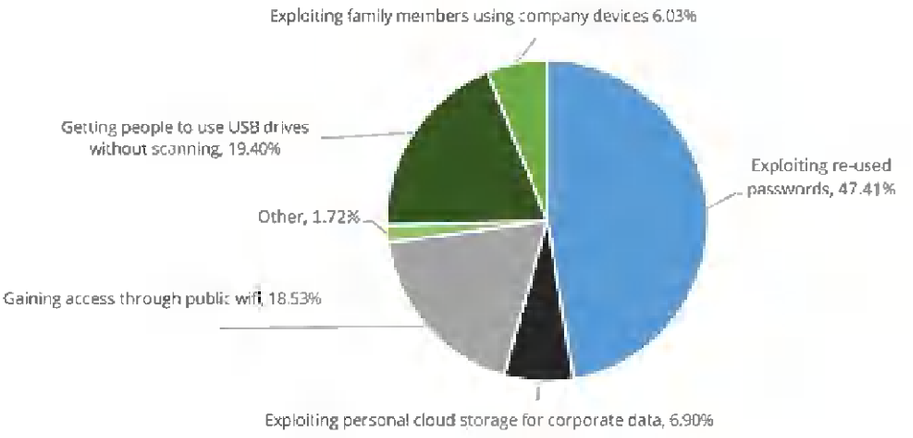

Fig. 3. Thycotic Black Hat 2018 Hacker Survey Report - "What risky behavior do you exploit the most?" [24]

Woo, Kim and Dominick (2009)

By analyzing the content of 462 defaced online pages in the English language, Woo, Kim, and Dominick investigated the motivations of hackers who defaced web pages. The motivations were categorized into two groups.

First, 'militant' impulses were confrontational and manifested as anti-outgroup reactions. More specifically, content was labelled militant when it alluded to nationalism, ethnicity, and religion, which were observed in 18% web pages examined and, the freedom of information and the prohibition of pornography were observed in 5% of the web pages examined [25].

"Pranking" motivations make up the second group. Prankster statements were found on 71% of the web sites examined. These statements brag about the hacker's abilities and skills (8%), impressing a romantic partner (2%), leaving a sign (24%) (e.g., "you were hacked by…"), or disparage the system administrator (4%) [25].

Goode and Cruise (2006)

Goode and Cruise examined the motivations of 28 software crackers by conducting an online survey. According to the results of this survey, the crackers were largely motivated by stimulation values. One of the most popular justifications was 'personal challenge'. At the same time, crackers stated that they would even crack if they would have to do it anonymously and solitary. Peer recognition, as well as monetary incentives, were not considered major motivators [26].

In a similar vein, crackers indicated they were neither motivated by public demand nor by personal need. Open-ended questions, on the other hand, revealed that crackers were aware that they were admired by others, but they disagreed on whether consumers of cracked software owed them gratitude [26].

Turgeman-Goldschmidt (2005)

Turgeman-Goldschmidt arranged the accounts reported by the 54 hackers he interviewed from the most to the least mentioned. Besides motivations to hack, he also noted factors that might persuade people to refrain from hacking and excuses, or justifications, to hack [27].

Only the reported motivations are considered in this study. Fun, thrill, and excitement are the most cited motivations, followed by curiosity, computer virtuosity, economic considerations, nosy curiosity, voyeurism, and revenge [27].

Fötinger and Ziegler (2004)

Fötinger and Ziegler analysed the intents of 599 people who had committed identity theft using data acquired through a questionnaire administered by the German Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA). Perpetrators who broke into the victims' computers exposed personal data relating to their internet accounts on online forums. As a result of the stolen data, others were able to access the internet at the expense of the victims, resulting in identity theft. Only six of the 599 respondents admitted to trespassing on victims' computers. None of the six people, however, admitted to posting the account information on the internet. As a result, the following results are based on responses from respondents who simply used 'publicly available' stolen details [28].

The two most frequently chosen drivers were: economic reasons (51.3%) and trial and error (33.1%). Among the less cited motivations (< 3%) were: fooling around, acceptance of the group, and competition [28].

5 Conclusion

In a world where cybercrime and malicious actions are as common as the sunrise, people substantially benefit in understanding more about the possible dangers of such useful tools as the Internet and technological devices. Human behavior is and will continue to be the source of many crimes. Taking advantage of one's ingenuity or lack of understanding on the topic will result in someone exploiting a service, blackmailing, extorting, or stealing someone's identity.

Considering the vast bulk of the aspects examined in this paper, we can conclude that the stream of crime is indeed increasing at a steady pace, either through the creation of new exploits, the use of misinformed people, poorly configured systems, outdated software, and the most common of all, human behavior, which leads to other types of threats such as extortion and blackmailing.

Nevertheless, not all is terrible, as organizations like INTERPOL and EUROPOL continue to move ahead and create methods to offer tools to start preventing most crimes, as well as national police forces throughout the globe being authorized to establish a unit to battle these dangers and respond faster and more efficiently.

It is essential to spread awareness as much as possible in order to continue preventing and minimizing damage. Reducing the amount of privacy violations and thefts must be a top priority; the data and statistics show that if nothing is done, more crimes will be committed.

References

1. Arora, B.: Exploring and analyzing internet crimes and their behaviours. Perspectives in Science. 8, 540–542 (2016).
2. Jain, N., Shrivastava, V.: Cyber crime changing everything – an empirical study. International Journal of Computer Application. 1, (2014). //reference incomplete
3. Nurse, J. R. C. Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit. (2018)
4. M3AAWG, http://www.maawg.org/, last accessed December 10, 2021
5. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 80, 973–993 (2014).
6. The cyber threat to UK business, https://www.ncsc.gov.uk/report/cyber-threat-uk-business last accessed December 1, 2021
7. Achten, A.: Identity Theft Resource Center to share latest Data Breach Analysis with U.S. Senate Commerce Committee; number of data breaches in 2021 surpasses all of 2020, https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-

analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/.
8. Reddy, G.N., Reddy, G.J.U.: A study of cybersecurity challenges and its emerging trends on latest technologies. International Journal of Engineering and Technology. 5, (2018).
9. Minei, E., Matusitz, J.: Cyberterrorist messages and their effects on targets: A qualitative analysis. Journal of Human Behavior in the Social Environment. 21, 995–1019 (2011).
10. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine. 30, 28–38 (2011).
11. Bada, M., Nurse, J.R.C.: The social and psychological impact of cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities. 73–92 (2020).
12. Gross, M.L., Canetti, D., Vashdi, D.R.: The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists. 72, 284–291 (2016).
13. Virtual rape is traumatic, but is it a crime?, https://www.wired.com/2007/05/sexdrive-0504/.
14. Kirwan, G., Power, A.: The Psychology of Cyber Crime. Advances in Digital Crime, Forensics, and Cyber Terrorism. (2012).
15. Nurse, J.R.: Cybercrime and you: How criminals attack and the human factors that they seek to exploit. The Oxford Handbook of Cyberpsychology. 662–690 (2018).
16. Norton's Cybercrime Report: The human impact reveals global cybercrime epidemic and our hidden hypocrisy, https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-report-human-impact-reveals-global-cybercrime.
17. Williams, M., Nurse, J.R., Creese, S.: Privacy is the boring bit: User Perceptions and Behaviour in the Internet-of-Things. 2017 15th Annual Conference on Privacy, Security and Trust (PST). (2017).
18. Nurse, J.R., Bada, M.: The group element of cybercrime: Types, dynamics, and criminal operations. The Oxford Handbook of Cyberpsychology. 690–715 (2018).
19. Madarie, R.: Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology. 11, (2017).
20. Sharma, R.: Peeping into a hacker's mind: Can criminological theories explain hacking? SSRN Electronic Journal. (2007).
21. Matthews, J., Goerzen, M.: Black hat trolling, white hat trolling, and hacking the attention landscape. Companion Proceedings of The 2019 World Wide Web Conference. (2019).
22. Juma'h, A.H., Alnsour, Y.: The effect of data breaches on company performance. International Journal of Accounting & Information Management. 28, 275–301 (2020).
23. Jouini, M., Rabai, L.B., Aissa, A.B.: Classification of Security Threats in Information Systems. Procedia Computer Science. 32, 489–496 (2014).
24. Thycotic Black Hat 2018 Hacker Survey Report, https://hosteddocs.emediausa.com/Thycotic-q4-18-2018-Black-Hat-Report.pdf.
25. Woo, H., Kim, Y., Dominick, J.: Hackers: Militants or Merry Pranksters? A content analysis of defaced web pages. Media Psychology. 6, 63–82 (2004).
26. Goode, S., Cruise, S.: What motivates software crackers? Journal of Business Ethics. 65, 173–201 (2006).
27. Turgeman-Goldschmidt, O.: Hackers' accounts hacking as a social entertainment. Social Science Computer Review. 23, 8–23 (2005).
28. Fötinger, C., Ziegler, W.: Understanding a hacker's mind - A psychological insight into the hijacking of identities. 1–48 (2004).

29. Klimburg-Witjes, N., Wentland, A.: Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. Science, Technology, & Human Values. 46, 1316–1339 (2021).
30. Benson, V.: Emerging cyber threats and cognitive vulnerabilities. Academic Press (2020).