Applying Neutralisation Theory to Better Understand Ransomware Offenders

Lena Connolly
Department of Computer Science
Zayed University
Abu Dhabi, UAE
alena.connolly@zu.ac.ae

Hervé Borrion
Department of Security and Crime Science
University College London
London, United Kingdom
h.borrion@ucl.ac.uk

Budi Arief
School of Computing
University of Kent
Canterbury, United Kingdom
b.arief@kent.ac.uk

Sanna Kaddoura
Department of Computer Science
Zayed University
Abu Dhabi, UAE
sanaa.kaddoura@zu.ac.ae

***Abstract*—The work presented in this paper investigates the crime of ransomware from the perspective of neutralisation theory. In particular, this research-in-progress paper aims to explore the feasibility of using neutralisation theory to better understand one of the key stakeholders in ransomware operations: the offenders. Individuals (including offenders) may employ techniques of neutralisation in order to justify their rule-breaking acts, and to diminish both the perceived consequences of their acts and the feeling of guilt. The focus of this work is on highly organised ransomware groups that not only conduct cyber attacks but also operate Ransomware-as-a-Service (RaaS) businesses. Secondary data was used in this research, including media interviews with alleged ransomware offenders. Data analysis is currently ongoing, but preliminary results show that ransomware offenders mainly use six neutralisation techniques to minimise the perceived impact and/or guilty feeling of their actions. These six neutralisation techniques are (1) denial of victim, (2) denial of injury, (3) claim of benefits, (4) claim of entitlement, (5) defence of necessity, and (6) claim of relative acceptability. The findings from this work can shed some light on the ransomware offending pathways, which in turn can be utilised to devise more effective countermeasures for combatting ransomware crime.**

Keywords—ransomware crime, neutralisation theory, countermeasures

INTRODUCTION

Ransomware continues to be one of the most harmful malware threats to individuals and organisations [1, 2]. Ransomware experienced an incredible evolution journey from primitive AIDS Trojan that emerged in 1989 to more sophisticated variants with advanced propagation capabilities, virtually unbreakable cryptography and the ability to steal data [3]. Ransomware is a form of modern transnational organised crime and a multi-billion-dollar industry, which keeps on growing [4]. Its operations are often run by so-called 'career criminals' who increasingly focus on more targeted attacks that require an extensive reconnaissance and advanced technical skills. Such an approach allows criminals to demand astronomical ransom payments. If the ransom is not paid, the consequences could include major disruption to critical infrastructure, loss of critical data and even company bankruptcy [5]. It is therefore essential to develop effective measures against ransomware. One of the concerning evolutions of ransomware is the emergence of *Ransomware-as-a-Service (RaaS)*. With RaaS, ransomware authors or developers are 'renting out' their ransomware kits to other threat actors (often known as 'ransomware affiliates') for a cut in the profit. As a consequence, sophisticated ransomware attack tools have become more readily available [6], making it easier for wannabe ransomware offenders to get in on the act, without needing to attain advanced technical skills first. In turn, such a proliferation of ransomware attack tools and ransomware operators increases the threat and potential damage that can caused by ransomware.

Ransomware is a crime and, as such, it is logical to analyse it from a criminological perspective. In understanding the various forms of misbehaviour, scholars from the field of environmental criminology employ a range of opportunity-based perspectives, including (but not limited to) *routine activity theory*, *situational action theory*, *rational choice theory* and *situational crime precipitators* (see, for example, references [7-9]). However, reference [10] argued that *neutralisation theory* can provide particularly pertinent insights into misbehaviour. Furthermore, reference [11] stressed that many criminals do not perceive criminal behaviour as acts of nonconformity, and neutralisation theory is an explanatory framework that provides reasoning in support of this finding.

Neutralisation theory has received a lot of attention among academic communities in general, and criminologists in particular (for detail, please see Section II of this paper, which provides a comprehensive literature review regarding the application of neutralisation theory in cybercrime). However, most of the existing research has focused on piracy with a handful of studies on sexting, cyberbullying and computer hacking (e.g., guessing passwords, gaining illegitimate access to a computer or network, and manipulating files or data) [12]. While this is a well-documented area, we have not found any study that investigated ransomware through the lens of neutralisation theory. In fact, there are only a handful of ransomware papers that investigated the threat of ransomware from a socio-technical perspective. Extant literature tends to focus primarily on technical measures, as discussed in [1], [13] and [14]. The present study is therefore important to address this gap. Moreover, the present study can also help us to learn more from 'career criminals' regarding their offending pathways.

A few attempts have been made to study criminals of higher-level keystone cybercrimes. Reference [15], for instance, studied online booter services, while reference [16] focused on a wider range of cybercriminals, including suppliers of DDoS as a service, malware distributors, bot shops' operators, and providers of services for web exploitation and account cracking. However, as far as we know, no study specifically focused on ransomware offenders. This is important because offenders' motivations to commit crime may depend on the type of the crime [12].

As such, the study presented in this paper aims to understand whether neutralisation theory applies to ransomware offenders. Assuming the answer is yes, we would also like to identify which neutralisation techniques are commonly used by ransomware offenders.

To answer these questions, we have been analysing data from several interviews (conducted by third-party media and cybersecurity organisations) with alleged ransomware offenders. Our work endeavours to addresses the aforementioned shortcomings in the current literature in several ways: (1) it focuses on a crime that has not been extensively studied from a socio-technical perspective; (2) it approaches the analysis through neutralisation theory, which has not been done before; (3) it uses data collected from actual (albeit alleged) ransomware offenders.

The specific focus of this work is on the members of ransomware gangs (including affiliates working for these gangs) that normally intend to commit data theft (in addition to encryption), which increases the chances of higher bounties from the victims.

The rest of this paper is organised as follows. Section II provides information about the theoretical framework behind neutralisation theory, including its relevance to cybercrime, as well as related work. Section III explains our research methodology, covering the sampling strategy and data analysis. Section IV highlights the preliminary results we have obtained so far. Finally, Section V concludes the paper and outlines study limitations.

THEORETICAL FRAMEWORK

Neutralisation Theory

Developed by Sykes and Matza in the 1950s, neutralisation theory posits that techniques are used to protect 'the individual from self-blame and the blame of others after the act' [17]. Effectively, individuals may utilise justifications in order to be freed from moral, ethical, and legal bindings [11]. Furthermore, reference [18] clarified that people use neutralisation techniques in order to justify participation in some form of wrongdoing and diminish both the consequences of their acts and the feeling of guilt. As reference [11, p.190] succinctly put it, 'persons employ verbal or cognitive techniques to convince themselves of the acceptability or appropriateness of their actions in a certain situation, regardless of the proscriptions of the dominant culture in place. Participation in the activity can then occur, and no deviant identity is assumed by the participant because of the neutralising process'.

Originally, Sykes and Matza proposed five techniques of neutralisation, including *denial of responsibility*, *denial of injury*, *denial of victim*, *condemnation of condemners* and *appealing to higher loyalties* [17]. In using the *denial of responsibility technique* ('it is not my fault'), the perpetrator places the blame on other factors or circumstances, which forced them to conduct an illegal activity. *Denial of injury* ('no harm resulted from my actions') is dismissing that a victim actually suffered serious consequences from their behaviour. The criminal claims that the victim deserved what they got relates to the utilisation of the *denial of victims* ('nobody got hurt') technique. *Appeal to higher loyalties* ('there is a greater and higher cause') is identified as prioritising the needs of family, friends and other important causes over following the law (e.g., loyalty to a criminal group is demonstrated by committing crime). Finally, *condemnation of condemners* ('how dare they judge me, considering how corrupt they themselves are') explains that the perpetrator shifts the focus from their criminal acts to the criminal behaviour of the potential victims by pointing out how they have victimised others and therefore deserve harm or mistreatment.

Sykes and Matza's five techniques of neutralisation [17] have been found to be relevant in understanding the justifications offenders use when committing various forms of delinquency, including shoplifting [19], illegal hunting [20], white-collar crime [21] and hired killing [22].

As research on neutralisation theory advanced, additional techniques, commonly referred to as supplementary, have been identified by academic community [12]. For instance, reference [23] discovered that individuals may commit delinquency acts if they believe their actions are necessary in certain situations. In such instances, the *defence of necessity* ('no other acceptable option is available to me') technique allows offenders to dismiss the feeling of guilt even if their behaviour is considered morally wrong. Reference [24] found that *metaphor of the ledger* ('if you weigh all of my good deeds against my bad deeds, you will see I am a decent person'), or one's belief that they have done more good than bad in their life, has been used by a professional fence to diminish guilt. Effectively, the offender compares their good deeds with the current questionable deed, thereby excusing this one particular instance of wrongdoing.

Reference [25] proposed three more neutralisation techniques, including *claim of normalcy*, *denial of negative intent* and *claim of relative acceptability*. In using *claim of normalcy* ('look, everyone is doing it, so how could it be wrong'), the criminal believes that the activity in question is one in which many others partake and therefore should not be considered criminal. When people acknowledge that criminal behavior took place, they can still escape reality by denying that they did not do it intentionally, which corresponds to the *denial of negative intent* ('I didn't intend to cause harm') technique. The *claim of relative acceptability* ('at least I am not a murderer or rapist; people engage in much worse activity than this') technique helps offender escape culpability by comparing their behaviour to more reprehensible deeds, thereby minimising the relative harmfulness of their acts.

In addition to *claim of normalcy*, reference [26] also investigated the *claim of entitlement* ('I deserve a reward') technique and found that white-collar criminals excuse their delinquency by claiming that most individuals engage in this behaviour and that they deserve to be occasionally rewarded. Reference [27] demonstrated that persons may excuse the act of sexting by using the *claim of benefits* technique ('my actions are beneficial for all involved parties'), where the perpetrator refutes an act's criminal status by identifying valued consequences of the act (e.g., in this particular research participants claimed that sexting helped them with their

relationships). Finally, reference [19] revealed the individual may use *postponement* ('I just do not think about it') to supress their guilt feelings by simply putting the act of crime out of their mind, so they can deal with it at a later time.

Neutralisation Theory and Cybercrime

A comprehensive literature review demonstrated that researchers have examined the relationship between cybercrime and techniques of neutralisation to understand the justification processes involved in online crime. However, most of scholarly research has focused on digital piracy (see [11], [28-33]), with some additional studies on sexting [27], cyberbullying [34] and computer hacking [35].

Referring to the original neutralisation theory, reference [12] summarised that, by and large, research on digital piracy demonstrates a strong support for *denial of injury* and *denial of victim* neutralisation techniques, and only mixed or moderate support for *denial of responsibility*, *condemnation of condemners*, and *appeal to higher loyalties*. The academic community has also examined the relationship between digital piracy and additional neutralisation techniques, including *defence of necessity* [36, 37], *metaphor of the ledger* [11, 37], *claim of normalcy* [11, 37], *claim of entitlement* [38] and *claim of relative acceptability* [38]. As with the original neutralisation theory, only mixed evidence was found in support of supplementary neutralisation techniques. For instance, reference [36] found modest support for the association of *defence of necessity* with digital piracy. In contrast, reference [37] concluded that *defence of necessity* and *claim of normalcy* are predictors of online piracy, but *metaphor of the ledger* is not.

Ransomware is a complex phenomenon that involves at least two types of crime: hacking and cyber extortion [39]. Considering the first one, reference [33] has argued that very limited work has focused on the use of neutralisation techniques in hacking. For instance, reference [40] found that software crackers do not deny responsibility for their actions and argue that some of their targets (i.e., vendors of expensive software) deserve to be victimised. According to reference [41], hackers not only refute the idea that victims are harmed, but also argue that their actions benefit others since they bring attention to security vulnerabilities in systems.

Furthermore, some offenders believe that even if victims incur financial losses, this is only temporary as they are eventually compensated by financial institutions [15]. Perpetrators that commit minor forms of hacking and use illegal software argue that computer intrusions are not as serious as other illegal acts [35, 42]. Hackers may deliberately target specific victims, especially if the victims are viewed as harming others [41]. This is particularly true for offenders who commit cyber-attacks for ideological, religious and political purposes [43, 44].

Research has also demonstrated that ideologically motivated hackers are often knowledgeable about technology, mistrust authorities and believe that information should be free and accessible [33]. Related to this, reference [44] found that hackers tend to deface websites to bring attention to a particular cause or search for government servers with the aim to disclose information that they believe people should have access to. Finally, reference [33] also examined the willingness of college students to deface websites and compromise financial and government servers and found strong evidence to support the relationships between neutralisation techniques and these cyber-attacks.

RESEARCH METHOD

Sampling Strategy

The study examined purposely selected ransomware groups (including the actors that are associated with these groups) that, not only conduct ransomware attacks, but also operate a RaaS model by selling their variants to other criminals to conduct attacks. Such groups represent a highly organised crime organisations and their members are commonly described as 'career criminals' [4]. These particular criminal groups commonly focus on committing more than one crime (which may include encryption, data theft, fraud, and cyber extortion) in a single attack, but mainly endeavour to steal data to significantly increase chances of successful extortion with a blackmail attempt [1]. The RaaS variants started emerging in 2019 and became particularly prevalent since 2020.

Nine documents published between November 2020 and December 2021 by various media and cybersecurity organisations were examined in this study. These organisations include Recorded Future, Cisco Talos Intelligence Group, New York Times, Flashpoint, KELA Cyber Intelligence Centre, Russian OSINT and Lenta.ru. These documents were found online via Google search with several keywords such as 'ransomware criminal interview' and 'ransomware offender interview'. We only considered documents containing data or excerpts of interviews with ransomware offenders involving the newest versions of ransomware that operate a RaaS model and normally steal data. All documents that met this criteria were included in this study.

Collectively, these documents provided rich and diverse information about offender motivation and justification. Some of them included interviews with alleged ransomware offenders, while others contained highlights from the interviews. One of the documents contained information from a ransomware group's dashboard and secret chats between group members. Some of the interviews were conducted, translated and transcribed by the same organisation, while others had more than one organisation involved for these activities. Two documents had a note informing readers that their interview had been lightly edited for clarity; the rest of the documents did not include any such specific details.

Regarding demographic information of participants, seven out of nine were Russian speakers (nationality was not specified), one participant was Ukrainian (language was not specified), and one document did not specify the native language of the interviewee. The documents we obtained were already translated in English. The participants claimed to be working with criminal groups including Avaddon, BlackMatter, Darkside, LockBit, Ransomex, REvil, Sodinokibi, TheDarkOverLord – either as contractors (i.e. 'affiliates') or permanent group members. Some participants shared their aliases with interviewers. Although interviewers referred to all participants as 'male', gender cannot be confirmed with certainty since interviews were conducted via chats and therefore interviewers could not see the participants in-person.

Data Analysis

Data analysis is currently ongoing, but some phases have been already completed. In the opening stage of the analytical process (Phase 1 – *open coding*), the body of data was segmented into discrete 'incidents' [46] or 'units' [47]. A data unit is defined as the 'smallest piece of information about something that can stand by itself, that is, it must be interpretable in the absence of any additional information other than a broad understanding of the context in which the inquiry is carried out' [47, p.345]. The goal of *open coding* is to systematically organise the data and uncover the essential ideas found in the data [48]. Each discrete unit of data received a label that represented a phenomenon. Altogether, 34 units (also referred as codes) were identified in our study.

The next phase (Phase 2 – *categorisation of incidents*) was approached with an open mind. Specifically, the intention was to look for both participant-driven and researcher-driven categories in order to sort the incidents of data from Phase 1 into these categories. The former would be derived from familiarity with the participants' customs and language, while the latter from a theoretical framework underpinning this study. Reference [49, p.153] explained the analytical importance of participant-driven themes: 'the actual words people use can be of considerable analytic importance as the 'situated vocabularies' employed provide valuable information about the way in which members of a particular culture organise their perceptions of the world, and so engage in the social construction of reality'.

Over the course of this analytical process (i.e., sorting out codes into categories), categories underwent various changes: while some of them were substantiated quickly, others were eliminated as irrelevant to the focus of inquiry; some were merged due to overlap or needed to be re-defined, and new codes emerged. Altogether, 10 categories were identified.

In the third phase (Phase 3 – *themes identification*), categories were grouped into themes. Interestingly, the results of this phase produced six themes (i.e., six neutralisation techniques relevant to ransomware crime), which already existed in the extant literature. Therefore, no new neutralisation techniques that are specifically relevant to ransomware crime were discovered in this exercise. All the existing definitions of neutralisation techniques were carefully examined to ensure that the categories were correctly placed within themes.

Additionally, we ensured that all categories and themes from Phases 2 and 3 were unique, which means that no data unit could fall between two groups nor fit into more than one group.

Research Rigour

Rigour in qualitative research, 'the means by which we attempt to show integrity and competence' [50], can be demonstrated via various techniques [51]. Reference [52], however, argued that the choice of the techniques to ensure the trustworthiness of research findings will depend on the context of the study and researchers should be allowed flexibility in selecting them.

In the context of this study, we decided to implement a multiple coder approach due to several papers indicating that definitions of some neutralisation techniques tend to overlap [53, 54]. Although the first coder studied the definitions of techniques identified in this study (i.e., relevant to ransomware crime) with caution, indeed, at times it was difficult to sort data under themes. Specifically, it seemed like some codes and categories belonged to more than one theme. Therefore, the decision was made to conduct a second round of coding (i.e., repeating Phases 1-3) to ensure the rigour in this research study. This phase is currently ongoing.

Once the second coder will complete the data analysis work, both coders will meet to discuss commonalities and differences in their results, in order to refine the coding system and, subsequently, the results of Phases 1-3.

Finally, Phase 4 will be concerned with the interpretation of results.

The Ethics Committee at [Anon University] approved this research. Although all study participants ensured their own anonymity, we carefully examined the documents to ensure that confidentiality of interviewees is respected as per ethical norms in research projects.

PRELIMINARY RESULTS

Preliminary results show that alleged ransomware offenders employ six neutralisation techniques to justify their criminal actions: *denial of victim*, *denial of injury*, *claim of benefits*, *claim of entitlement*, *defence of necessity* and *claim of relative acceptability*. Although these findings still need to be confirmed through the second round of coding, several quotes evidencing the data analysis results are presented below. For instance, throughout the interviews, some study participants assume that victims generate enough revenue to cover the ransom and therefore such attacks would not be impacting them (*denial of injury*):

> "*…Our business does not harm individuals and is aimed only at companies, and the company always has the ability to pay funds and restore all its data…*"

In using the *denial of victim* technique, alleged offenders explain their motives by claiming that the violated party deserved everything that happened:

> "*We prefer to attack those who are like us – 'business sharks'*".

> "*…In general, if there is an understanding [with victims] that you have to pay, no other options, but not as much. We will find a common language. But if we get delusional messages like, "There is no money" or, "We will pay one-tenth," you have no one to blame but yourself [concessions are not possible]*".

Furthermore, suspected perpetrators tend to believe that their actions produce benefits (i.e., *claim of benefits*). In this particular instance the alleged offender claims the benefits to society:

> "*We do not deny that business is destructive, but we look deeper. As a result of these problems, new technologies are developed and created. If everything was good everywhere, there would be no room for new development*".

Results also demonstrate that study participants *claim entitlement* to rewards because they deserve them:

> "*There is one life and we take everything from it*".

Some participants use a *claim of relative acceptability* technique to escape culpability by comparing their behaviour

to more reprehensible deeds, thereby minimising the relative harmfulness of their acts:

> "*We do not attack healthcare, education, charitable organizations, social services* […] *We have a negative attitude towards ransomware gangs that encrypt healthcare and educational institutions*".

Finally, the alleged perpetrators employ a *defence of necessity* technique claiming that in current circumstances no other option is available to them:

> "*In the West, I would probably work in white [hat security] and earn easily*".

CONCLUSION AND STUDY LIMITATIONS

We would like to note that although valuable, this study is not without limitations due to the use of secondary data. First, this leaves the question of data accuracy open. Furthermore, secondary data inevitably lead to some voids. For instance, we do not know the very specifics of ransomware groups' operations (i.e., some of them may include nationalistic dimension and therefore see victims as adversaries deserving the harm, while others pursue purely financial interests). Finally, there is a risk that limited data were collected since we are not in a position to determine a point of sufficient theoretical saturation. Nonetheless, it is important to note that collecting data on cybercrime from actual offenders is extremely difficult [12], and even more so from ransomware offenders since they rarely get arrested and prosecuted [55]. Therefore, although incomplete, such data are valuable.

In summary, this research is significant because the knowledge of what neutralisation techniques ransomware offenders employ to commit crime will allow us to suggest preventive measures for policymakers that can potentially reduce ransomware crime. In the final phase of this study we also endeavour to suggest implications for research and theory and suggest future research directions.

ACKNOWLEDGMENTS

As part of the open-report model followed by the Workshop on Attackers & CyberCrime Operations (WACCO), all the reviews for this paper are publicly available at https://github.com/wacco-workshop/WACCO/tree/main/WACCO-2023.

REFERENCES

[1] M. Lang, L. Connolly, P. Taylor and P.S. Corner, "The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks," Digital Threats: Research and Practice, 2022.

[2] C. Brierley, B. Arief, D. Barnes and J. Hernandez-Castro, "Industrialising blackmail: Privacy invasion based IoT ransomware", In 26th Nordic Conference on Secure IT Systems (NordSec 2021), pp. 72-92, 2021.

[3] L. Connolly, M. Lang, P. Taylor and P.S. Corner, "The evolving threat of ransomware: From extortion to blackmail," pre-print, 2021.

[4] D. Wall, "The transnational cybercrime extortion landscape and the pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending," European Law Enforcement Research Bulletin, 22, 2021.

[5] L. Connolly and H. Borrion, "Reducing ransomware crime: Analysis of victims' payment decisions, Computers & Security, vol. 119, 2022.

[6] G. Hull, H. John and B. Arief, "Ransomware Deployment Methods and Analysis: Views from a Predictive Model and Human Responses", Crime Science 8(2), 2019.

[7] J. Basamanowicz and M. Bouchard, "Overcoming the warez paradox: Online piracy groups and situational crime prevention," Policy & Internet, vol. 3, pp. 1-25, 2011.

[8] A. Jordanoska, "The social ecology of white-collar crime: Applying situational action theory to white-collar offending", Deviant Behavior, vol. 39, pp.1427-1449, 2011.

[9] T.C. Pratt, K. Holtfreter and M.D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory", Journal of Research in Crime and Delinquency, vol. 47, pp.267-296, 2010.

[10] L.C. Harris, "Breaking lockdown during lockdown: A neutralization theory evaluation of misbehavior during the Covid 19 pandemic", Deviant Behavior, vol. 43 no. 7, pp.765-779, 2022.

[11] S. Hinduja, "Neutralization theory and online software piracy: An empirical analysis", Ethics and Information Technology, vol. 9 no. 3, pp. 187-204, 2007.

[12] R. Brewer, S. Fox and C. Miller, "Applying the techniques of neutralization to the study of cybercrime", The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp.547-565, 2020.

[13] L. Connolly and D. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures, Computers & Security, Vol. 87, pp.1-18, 2019.

[14] T. McIntosh, A.S.M. Kayes, Y.P.P. Chen, A. Ng and P. Watters, "Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future direction", ACM Computing Surveys (CSUR), 54(9), 1-36, 2021.

[15] A. Hutchings and R. Clayton, "Exploring the provision of online Booter services", Deviant Behavior, vol. 37, pp. 1163–1178, 2016.

[16] S. Pastrana, D.R. Thomas, A. Hutchings and R. Clayton, "CrimeBB: Enabling cybercrime research on underground forums at scale", 2018 World Wide Web Conference, pp. 1845-1854, 2018.

[17] G. Sykes and D. Matza, "Techniques of neutralization: A theory of delinquency, American Sociological Review, 22, pp. 664–670, 1957.

[18] J. Mitchell and R.A. Dodder, "An examination of types of delinquency through path analysis", Journal of Youth and Adolescence vol. 9, no. 3, pp. 239–248, 1980.

[19] P. Cromwell and Q. Thurman, "The devil made me do it: Use of neutralizations by shoplifters", Deviant Behaviour, vol. 24, no. 6, pp. 535–550, 2003.

[20] E. Von Essen, H.P. Hansen, H. Nordström Källström, M. N. Peterson and T.R. Peterson, "Deconstructing the poaching phenomenon: A review of typologies for understanding illegal hunting", British Journal of Criminology, vol. 54, no. 4, pp. 632-651, 2014.

[21] J. McGrath, "Self-deception as a technique of neutralisation: An analysis of the subjective account of a white-collar criminal", Crime, Law and Social Change, vol. 75 no. 5, pp.415-432, 2021.

[22] K. Levi, "Becoming a hit man: Neutralization in a very deviant career", Urban Life, vol. 10, no. 1, pp. 47–63, 1981.

[23] W.W. Minor, "Techniques of neutralization: A reconceptualization and empirical examination", Journal of Research in Crime and Delinquency, vol. 18, no. 2, pp. 295–318, 1981.

[24] C. B. Klockars, The Professional Fence. Free Press, New York, 1974.

[25] S. Henry, Degrees of Deviance, Student Accounts of their Deviant Behavior. Sheffield Publishing, Salem, 1990.

[26] J. W. Coleman, The criminal Elite: The Sociology of White Collar Crime. St. Martin's Press, 1985.

[27] D.G. Renfrow and E.A. Rollo, "Sexting on campus: Minimizing perceived risks and neutralizing behaviors", Deviant Behavior, vol. 35, no. 11, pp.903-920, 2014.

[28] G.E. Higgins, S.E. Wolfe and C.D. Marcum, "Music piracy and neutralization: A preliminary trajectory analysis from short-term longitudinal data", International Journal of Cyber Criminology, vol. 2, no. 2, 2008.

[29] J.R. Ingram and S. Hinduja, "Neutralizing music piracy: An empirical examination", Deviant Behavior, vol. 29, no. 4, pp.334-366, 2008.

[30] T.J. Holt and H. Copes, "Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates", Deviant Behavior, vol. 31, no. 7, pp.625-654, 2010.

[31] C.D. Marcum, G.E. Higgins, S.E. Wolfe and M.L. Ricketts, "Examining the intersection of self-control, peer association and neutralization in explaining digital piracy", Criminology, Criminal Justice, Law & Society, vol. 12, no. 3, 2011.

[32] J.F. Popham and C. Volpe, "Predicting moral disengagement from the harms associated with digital music piracy: An exploratory, integrative test of digital drift and the criminal interaction order", International Journal of Cyber Criminology, vol. 12, pp. 133–150, 2018.

[33] A. M. Bossler, "Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks", American Journal of Criminal Justice, vol. 46, no. 6, pp.911-934, 2021.

[34] S. Zhang, L. Yu, R.L. Wakefield and D.E. Leidner, "Friend or foe: Cyberbullying in social network sites", ACM SIGMIS Database: the DATABASE for Advances in Information Systems, vol. 47, no. 1, pp.51-71, 2016.

[35] R.G. Morris, "Computer hacking and the techniques of neutralization: An empirical assessment." In T. J. Holt & B. H. Schell (Eds.), Corporate hacking and technology-driven crime: Social dynamics and implications, pp. 1-17, Hershey, PA: IGI-Global, 2011.

[36] R.G. Morris and G.E. Higgins, "Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates", Criminal Justice Review, vol. 34, pp. 173–195, 2009.

[37] J.L. Smallridge and J.R. Roberts, "Crime specific neutralizations: An empirical examination of four types of digital piracy", International Journal of Cyber Criminology, vol. 7, pp. 125–140, 2013.

[38] R.J. Maratea, "Screwing the pooch: Legitimizing accounts in a zoophilia on-line community", Deviant Behavior, vol. 32, pp. 918–943, 2011.

[39] L. Connolly and H., Borrion, "Your money or your business: Decision-making processes in ransomware attacks, International Conference on Information Systems, 2020.

[40] S. Goode and S. Cruise, "What motivates software crackers?" Journal of Business Ethics, vol. 65, no. 2, pp.173-201, 2006.

[41] A. Hutchings, Hacking and Fraud in Global Criminology: Crime and Victimization in a Globalized Era, CRC Press, 2013.

[42] Y.T. Chua and T.J. Holt, "A cross-national examination for the techniques of neutralization to account for hacking behaviors", Victims & Offenders, vol. 11, pp. 534–555, 2016.

[43] T.J. Holt, J.D. Freilich and S.M. Chermak, "Exploring the subculture of ideologically motivated cyber-attackers", Journal of Contemporary Criminal Justice, vol. 33, pp. 212–233, 2017.

[44] T.J. Holt, M. Kilger, L. Chiang and C. Yang, "Exploring the correlates of individual willingness to engage in ideologically motivated cyberattacks", Deviant Behavior, vol. 38, pp. 356–373, 2017.

[45] T.J. Holt, M. Kilger, L. Chiang and C.S. Yang, "Exploring the behavioral and attitudinal correlates of civilian cyberattacks. In Social Networks, Terrorism and Counter-terrorism, pp. 128-151). Routledge, 2015.

[46] B.G. Glaser and A.L. Stauss, The Discovery of Grounded Theory. Chicago, Aldine, 1967.

[47] Y. Lincoln and E. Guba. Naturalistic Inquiry. Beverly Hills, California, Sage Publications Inc, 1985.

[48] R. Baskerville and J. Pries-Heje, "Short cycle time systems development", Information Systems Journal, vol. 14 no. 2, pp. 237-264, 2004.

[49] M. Hammersley and P. Atkinson, Ethnography: Principles and Practice. London: Tavistock, 1983.

[50] R. Aroni, D. Goeman, D., K. Stewart, S. Sawyer, M. Abramson and F. Thein, "Concepts of rigour: When methodological, clinical and ethical issues intersect", In Association for Qualitative Research Conference, Melbourne, 1999.

[51] R.S. Barbour, "Checklists for improving rigour in qualitative research: A case of the tail wagging the dog?" British Medical Journal, vol. 322, no. 1, pp. 115-117, 2001.

[52] L. Berends and J. Johnston, "Using multiple coders to enhance qualitative analysis: The case of interviews with consumers of drug treatment", Addiction Research & Theory, vol. 13, no. 4, pp.373-381, 2005.

[53] W.A. Stadler and M.L. Benson, "Revisiting the guilty mind: The neutralization of white-collar crime", Criminal Justice Review, vol. 37, no. 4, pp.494-511, 2012.

[54] G. Enticott, "Techniques of neutralising wildlife crime in rural England and Wales", Journal of Rural Studies, vol. 27 no. 2, pp.200-208, 2011.

[55] R. Iyengar, "Why it's so difficult to bring ransomware attackers to justice", CNN, 2021, available online: https://edition.cnn.com/2021/07/08/tech/ransomware-attacks-prosecution-extradition/index.html [Accessed October 2022]