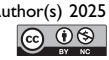
Special Issue

European Journal of Criminology

Ransomware crime through the lens of neutralisation theory

European Journal of Criminology
1–23



DOI: 10.1177/14773708251320464
journals.sagepub.com/home/euc


Lena Yuryna Connolly
Zayed University, United Arab Emirates

Hervé Borrion
University College London, UK

Budi Arief
University of Kent, UK

Abstract

This study examines ransomware crime through the lens of neutralisation theory, and explores techniques used by alleged offenders to justify their involvement in ransomware attacks. This work focuses on highly organised ransomware groups that not only conduct attacks but also operate as Ransomware-as-a-Service businesses. The interview data ($n = 9$) used in this research were collected by several media and cyber security companies. Drawing on Kaptein and Van Helvoort model of neutralisation techniques, we discovered that interviewees – reported ransomware offenders – distorted the facts ($n = 5$) and negated societal norms ($n = 8$). Less common, some interviewees admitted breaking norms, but they rejected responsibility by blaming the circumstances ($n = 8$) or their own shortcomings ($n = 3$). These results offer new insights that can support the development of counter-narratives.

Keywords

Cybercrime community, neutralisation theory, offender justifications, ransomware

Corresponding author:
Lena Yuryna Connolly, College of Technological Innovations, Zayed University, Abu Dhabi, United Arab Emirates.
Email: lena.connolly@gmail.com

Introduction

Ransomware is one of the most significant cybercrime types in the world, affecting both public- and private-sector organisations (Europol, 2023). This form of crime involves encrypting someone's data and holding it hostage until they pay a ransom. Lately, organisations have improved backup practices, leading to tactical displacement: Lang et al. (2023) explain that hackers not only encrypt but also steal data.

Organised crime groups (or Ransomware-as-a-Service - RaaS) operators who not only conduct attacks but also sell the malware) that are believed to be behind some of these ransomware attacks (RTF, 2022) share characteristics with legitimate businesses. Their operations are complex and systematic with clearly defined roles and responsibilities (Matthijsse et al., 2023; Meland et al., 2020; O'Kane et al., 2018). Internal business processes include technical operations such as malware development, sales and spread (i.e., distributors who infect victims' devices) (Alwashali et al., 2021; Meland et al., 2020) as well as managerial operations, including hiring and firing internal and external personnel, providing training, and utilising marketing to increase brand reputation, which potentially motivated some of our interviewees to step out of hiding and speak about their activities. RaaS operators also outsource various services in order to obtain information about vulnerabilities, gain initial access to the victim's network, host a website with a rogue hosting provider, and launder criminal proceeds. RaaS operators may also use the services of darknet marketplaces to assist in malware sales (Meland et al., 2020). Using crime script analysis, Matthijsse et al. (2023) represented the complexity of ransomware operations by identifying eight scenes necessary for a ransomware ecosystem to exist: (1) *preparation* that involves (a) forming collaborations, (b) setting up necessary infrastructure, and (c) developing in-house malware or purchasing it from alternative suppliers; (2) *select victim,* which can be opportunistic or targeted; (3) *gain access* to victim's system or network; (4) *infection* of as many systems as possible through various means, such as creating backdoors, stopping anti-virus services, elevating privileges, enabling lateral movement and deleting backups; (5) *encryption* of data and systems; (6) *doing,* which involves (a) extortion of victim by displaying the ransom demand, (b) communication between the victim and the attacker, (c) cash-in through a ransom collection if the victim decides to pay, and (d) emancipation, which incorporates a decryption of files if the attacker decides to release a decryption key; (7) *post-condition* that encompasses (a) money laundering and cash-out via placing, layering or integrating bitcoin into other wallets, other cryptocurrency systems or services or the traditional economy and (b) payment to collaborators and reinvestment into ransomware campaigns; and (8) *exit* where cybercriminals may exit business because they are caught by law enforcement or they made enough money. One common denominator in all these activities is the relentless effort to avoid detection using proxy servers and virtual private networks to conceal real IP addresses, Tor network and encryption to ensure anonymous communication; log manipulation and fileless malware to ensure no digital footprints are left on the victim's network; and the use of cryptocurrencies for anonymous payments (Huang et al., 2019). As such, ransomware groups do not exist in isolation; they are part of a much bigger cybercrime ecosystem, making them particularly resilient to disruptions (Europol, 2023). Yet, at the centre of each crime is an individual who chooses to engage in malicious activities.

Understanding how individuals justify their engagement to themselves and to others can offer valuable information to start developing offender-focused prevention measures.

In this research, we examine narratives from individuals who claimed to be ransomware offenders through the lens of neutralisation theory. We believe our study makes three valuable contributions: (1) we approach this topic from a point rooted in social science, while most research on ransomware is focused on the technological aspects of the attack (Connolly et al., 2023), with the exception of several studies analysing ransomware from a social perspective, such as Connolly et al. (2020), Hoevel (2024), Matthisse et al. (2023), Meurs et al., 2022; (2) to the best of our knowledge, this is the first time this problem is analysed using neutralisation theory; and (3) the results add to the very limited body of knowledge on organised cybercrimes. Given that ransomware offenders tend to operate anonymously, interview data is limited (Maimon and Louderback, 2019).

In the initial phase of this work, we have used the original theory of neutralisation proposed by Sykes and Matza (1957). However, as data analysis proceeded, we realised that the five original neutralisation techniques were not sufficiently granular to represent all the arguments used by ransomware actors in detail. Accordingly, we considered 'supplementary' techniques that have been proposed subsequently (Brewer et al., 2020). Our preliminary findings suggested that alleged ransomware actors employ six techniques of neutralisation, including two original techniques – *denial of victim* and *denial of injury*, and four supplementary – *claim of benefits*, *claim of entitlement*, *defence of necessity*, and *claim of relative acceptability* (Connolly et al., 2023).

Although the extant literature offers a considerable amount of supplementary techniques, they vary in terms of granularity, and many overlap with each other. Fritsche (2002: 485) argued that collectively these supplementary techniques 'do not offer a theoretically sound taxonomy, nor an exhaustive list', which can lead to inconsistent research findings (Maruna and Copes, 2005). Furthermore, Brewer et al. (2020) cautioned that the findings from existing cybercrime research must be interpreted carefully due to the aforementioned overlap, and they called for the adoption of methods that can clearly distinguish between the different neutralisation techniques. Kaptein and Van Helvoort (2019) recently proposed a new model. Using both deductive and inductive approaches, they searched for neutralisation techniques that have been identified in the academic and professional literature and organised them in a logical and systematic way. Leveraging their work, we endeavoured to identify and classify neutralisation techniques adopted by reported ransomware actors using their model. We found nine neutralisation techniques relevant to ransomware crime (i.e., three more than in our initial study). In addition, the granularity of the model allowed us to reveal distinct attributes for each technique. Such detailed findings provided us with a deeper understanding of the reasons invoked by offenders to commit ransomware crime.

Theoretical framework

Neutralisation theory

The theory of neutralisation, proposed by Sykes and Matza (1957: 666), suggests that individuals employ strategies that shield them 'from self-blame and the blame of others after the act'. Neutralisation techniques help them rationalise engagement in

wrongful behaviour, diminishing both the consequences of the actions and the burden of guilt. Hinduja (2007) surmised that this allows them to partake in rule-breaking activities without adopting a deviant identity and, thus, disregard societal norms. The five original techniques of neutralisation proposed by Sykes and Matza (1957) are *denial of responsibility* (i.e., the perpetrator shifts the blame to other factors, circumstances or people), *denial of injury* (i.e., they disregard the impact of the crime on the victim), *denial of victim* (i.e., the victim received what was warranted), *appeal to higher loyalties* (i.e., the offender claims that the needs of other people or causes are more important than obeying the law), and *condemnation of condemners* (i.e., the perpetrator redirects their attention from their own criminal actions to the victim's conduct). As research on neutralisation theory gained momentum, numerous supplementary techniques were developed by various scholars (see Connolly et al., 2023, for a review of the literature). Neutralisation techniques have been discovered to be applicable to a wide range of criminal activities such as shoplifting (Cromwell and Thurman, 2003), illegal hunting (Von Essen et al., 2014), white-collar crime (McGrath, 2021), and cybercrime (Hinduja, 2007; Popham and Volpe, 2018; Renfrow and Rollo, 2014) (n.b., additional literature is discussed in the findings section against each neutralisation technique found to be relevant to ransomware crime in this study). Outside peer-reviewed literature, we found several blogs written by researchers from Orange Cyberdefense (e.g., Dimitrievski et al., 2023a, 2023b; Ridley and Selck-Paulsson, 2022, 2023a, 2023b; Selck-Paulsson and Ridley, 2022) that demonstrate the link between neutralisation techniques and alleged ransomware offenders.

Kaptein and Von Helvoort (2019)'s model comprises four levels. The highest level specifies two broad categories: *denying deviant behaviour* ('it is not deviant') and *denying responsibility* ('I am not responsible for it'). Each of these categories is further divided into two sub-categories. Particularly, deviant behaviour can be denied through (I) *distorting the facts* ('it is not the truth') and (II) *negating the norm* ('it is not decisive'). When distorting the facts, individuals misrepresent them to themselves or to others, so the violation of the norm does not exist anymore. Essentially, people change their reality and create an illusion that no violation occurred by changing the description of the event. When negating the norm, the facts are not distorted, but the norm applicable to the situation is being refuted. People can create a new norm that would be applicable to the situation, so the old norm is neglected and subsequently the deviant behaviour is denied. Furthermore, when denying responsibility (i.e., the second broad category), individuals can (III) *blame the circumstances* through externalising the blame ('It is beyond my control') and by (IV) *hiding behind oneself*, where instead of blaming the circumstances, individuals reduce or diminish responsibility by hiding behind their own imperfect intentions, capabilities, and knowledge. The four subcategories further extend to 12 neutralisation techniques – each sub-category includes three techniques (the model's third level). Finally, the fourth level of the model includes 60 sub-techniques – five per each technique. The findings section offers a detailed description of techniques and sub-techniques identified in this research.

Kaptein and Von Helvoort (2019: 1263) argue that these categories are exclusive and exhaustive. They note that the techniques are associated with different levels of responsibility. Denying deviant behaviour, for example, is safer than denying responsibility

because one admits less guilt when using the former and has more neutralisation options available to them. Furthermore, when people deny deviant behaviour, it is safer to distort the facts rather than negate the norms because when the facts are changed and no norm is broken, there is no reason to neutralise someone's behaviour by negating the norm. However, when the facts cannot be changed, people acknowledge the facts but aim to modify the existing norm to excuse their behaviour. When deviant behaviour cannot be denied, however, it is safer to shift responsibility to circumstances before individuals admit the lack of self-control. Essentially, the model commences with neutralisations in which people distort the facts, asserting that no crime took place, and culminates with individuals acknowledging the occurrence of the crime and even the harm caused, all the while contending that they are mere humans and hence cannot be held responsible for their actions. With such granularity, the model was deemed highly appropriate to understand how offenders justify their involvement in ransomware attacks.

Method

Data

In selecting applicable participants, we focused on alleged members of ransomware groups that not only conduct ransomware attacks but also operate RaaS model by selling their variants to others. Interview data used in this study was collected by three media and four cyber intelligence organisations (Table 1 and Supplemental File A) and is openly available on the internet. Although the use of primary data would be preferable, arranging interviews with ransomware offenders is challenging due to the nature of their business (i.e., anonymity is the cornerstone of their operations). Working with secondary data, we could not validate the authenticity of some interviews; we relied on the reputation of the companies that published these interviews and claimed that these interviewees were ransomware offenders.

The search for interview data involved entering specific keywords (including 'ransomware criminal interview', 'ransomware offender interview' and 'ransomware crime interview') in the Google search engine. From the results, we selected nine documents (that fit our criteria) published between November 2020 and December 2021. These include six interview transcripts with reported offenders, two highlights from the interviews, and a report containing information from a ransomware group's dashboard and secret chats between group members. Published in English, these documents offer information about the motives and justifications of these offenders. Some interviews were conducted, translated and published by the same organisation, while others were conducted by one organisation and translated and published by another (Supplemental File A). Two documents contain a notice informing readers that an interview had undergone slight editing for clarity. To ensure results reproducibility, we provided links to the files in Table 1.

Table 2 contains demographic information about the interviewees ($n = 9$). One interviewee reported to be Ukrainian; seven others were identified as Russian speakers; and no information was available about the nationality or language of the last one. Two interviewees claimed to be contractors working for various ransomware groups, while the seven others worked only for one ransomware group at the time.

Table 1. The data used in the study.

Doc No and links	Interview date	Publication date	Publication form	Organisations involved in the interview process	Note on edits by interviewers/ publishers
1 Link	Not specified	September 2021	Interview transcript	Lenta.ru and Flashpoint	The interview has been lightly edited for clarity
2 Link	Not specified	February 2021	Analysis report (i.e., highlights from original article)	Recorded Future	Not specified
3 Link	Not specified	December 2021	Interview transcript	Recorded Future	Not specified
4 Link	September 2020, spanning a few weeks	January 2021	An article with both highlights and interview quotes	Cisco Talos Intelligence Group (CTIG)	Not specified
5 Link	Not specified	August 2021	Interview transcript	Russian OSINT; KELA Cyber Intelligence Center	Not specified
6 Link	Not specified	October 2021	Interview transcript	Recorded Future	Not specified
7 Link	Not specified	November 2020	Interview transcript	Recorded Future	The interview has been lightly edited for length and clarity
8 Link	Not specified	March 2021	Interview transcript	Recorded Future	Not specified
9 Link	Not specified	December 2021	A media article with quotes from DarkSide's secret chats and some information from their dashboard	*The New York Times*	Not specified

Data analysis

Two researchers, referred to as R1 and R2, conducted the analysis in six phases (Figure 1). In Phase 1 (*familiarisation*), R1 read all nine documents multiple times to become familiar with the data. In Phase 2 (*deductive open coding*), R1 extracted 46 quotes that seemed to confirm that neutralisation techniques were being used by their authors. Following Kaptein and Von Helvoort (2019) framework, R1 and R2 then drew a list of criteria (e.g., classification question) that could facilitate the identification of neutralisation techniques. For instance, the

Table 2. Interviewee information.

Document (D) No/ Interviewee (I) No and alias	Ransomware group(s)	Interviewee role	Interviewee nationality and language
D1/I1, 'Antivirus'	REvil and other ransomware groups	Contractor working for several ransomware groups	Unknown, Russian
D2/I2, 'Bassterlord'	Sodinokibi, LockBit, Avaddon, and Ransomex	Contractor working for several ransomware groups	Ukrainian, Unknown
D3/I3, no alias provided	BlackMatter	Team member	Unknown, Russian
D4/I4, 'Aleks'	LockBit	Team member	Unknown, Russian
D5/I5, no alias provided	LockBit	Team member	Unknown, Russian
D6/I6, no alias provided	LockBit	Team member	Unknown, Russian
D7/I7, no alias provided	TheDarkOverlord	Team member	Unknown, Unknown
D8/I8, 'Unknown'	REvil	Team member	Unknown, Russian
D9/I9, 'Woris'	DarkSide	Team member	Unknown, Russian

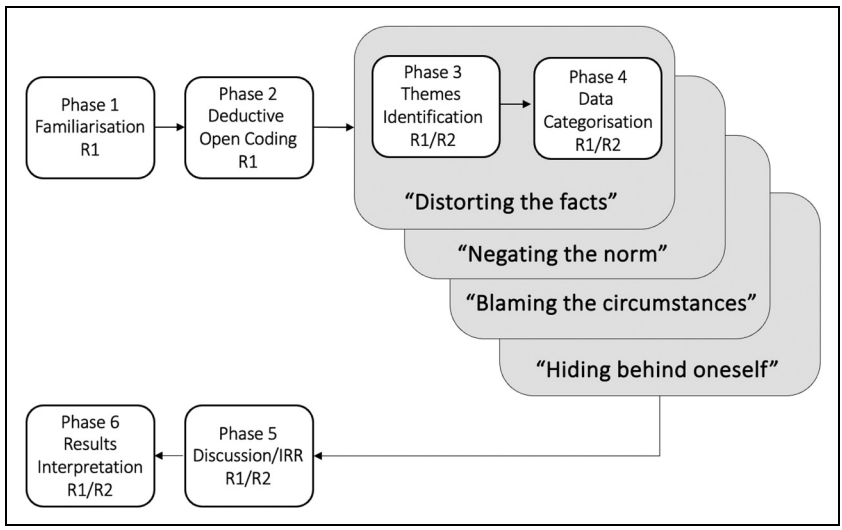


Figure 1. Data analysis.

question 'Did the interviewee suggest anything about the truth not existing or being too difficult to determine?' was used to decide if a quote was indicative of the *nuancing the facts* technique. For greater reliability, the researchers often reused sentences and examples from

Table 3. Neutralisation techniques and sub-techniques (greyscale version).

	Techniques											
Sub-techniques	1	2	3	4	5	6	7	8	9	10	11	12
	1	6	11	16	21	26	31	36	41	46	51	56
	2	7	12	17	22	27	32	37	42	47	52	57
	3	8	13	18	23	28	33	38	43	48	53	58
	4	9	14	19	24	29	34	39	44	49	54	59
	5	10	15	20	25	30	35	40	45	50	55	60

Note: White (no colour) cell – technique/sub-technique was not found to be relevant to ransomware crime in this study.
Gray cell – technique/sub-technique was found to be relevant to ransomware crime in this study.

the original publication. For example, Kaptein and Helvoort's illustrative expression 'It is my business, not yours' was preferred over the lengthier description of the corresponding sub-technique (*reduction to taste*, here).

As explained above, the neutralisation framework that guided our work consists of four sub-categories with three neutralisation techniques each. R1 and R2 independently ascertained if the 46 quotes matched the first sub-category ('Distorting the fact' in the *theme identification* phase; and if so, proceeded with the *data categorisation* phase, where they looked for the most relevant technique within the sub-category. After completing this task independently, they then met to compare and discuss the results. The *theme identification* and *data categorisation* processes were repeated for the second sub-category ('Negating the norm') and its techniques, and then the third ('Blaming the circumstances') and fourth ('Hiding behind oneself') sub-categories (Figure 1). Classification requires not only understanding but also memorising the techniques and their nuances, which was challenging given the complexity of the framework. By concentrating on one sub-category at a time, the researchers were able to reduce the cognitive workload, which likely improved classification accuracy and consistency. In Phase 5, R1 and R2 concluded that 14 quotes did not contain any evidence of neutralisation. The remaining 32 quotes were assigned a unique number to simplify the presentation of results (Supplemental File B). The results of individual coding indicated that both researchers agreed on neutralisation techniques used by interviewees in 48 instances and disagreed in 18 instances (Supplemental File C). The researchers discussed the cases where disagreement occurred and reached a consensus (Supplemental File D). Data analysis was concluded with Phase 6, which concerned the interpretation of results.

Findings

Nine neutralisation techniques and 19 sub-techniques were identified in the interviews (Table 3). *Denial of criminal behaviour* (Techniques 3, 4, 5 and 6) was found in 39 quotes ($n = 9$ interviewees); and *denial of responsibility* (Techniques 7, 8, 9, 11 and 12) in 16 quotes ($n = 8$ interviewees) (Supplemental File E).

Distorting the facts

Kaptein and Von Helvoort (2019) explain that *distorting the facts* can be done using three neutralisation techniques: (1) nuancing, (2) denying, and (3) inventing facts. None of the quotes were found to relate to the first two techniques, but several show that the interviewees tend to invent facts about the crime, which helps them reduce guilt.

Inventing new facts (Technique 3). When inventing new facts, the alleged offenders created a new reality, so the violated norm no longer (fully) applies. Five interviewees (Quotes (Q): 5, 9, 13, 20, 22, 27, 28) invented facts about some aspects of their criminal activities (sub-technique 14: the invention of circumstances). Some, for instance, diminished the severity of the crime by asserting that ransom payments, however large, are inconsequential to the victims (Q: 9, 27, 22):

> The company always has the ability to pay funds and restore all its data. (Interviewee 3)

Others made general statements about companies' investments in cyber security, before suggesting that these attacks are the natural consequence of their poor decisions (Q: 20, 28). Interviewee 6 fantasised that all organisations have means to pay the ransom:

> There are no companies without money [that cannot pay a ransom]. (Interviewee 6)

Kaptein and Von Helvoort (2019) explain that when *inventing new facts*, individuals argue that there is more happening than what is immediately apparent and the line between reality and fiction becomes unclear. People may construct a fictional realm as a response to the overwhelming nature of the actual world. For example, Scully and Marolla (1984) discovered that rapists engage in fantasies where their victims explicitly or indirectly express a desire to be victimised. This could indicate that those responsible for ransomware offences understand the negative impact of their actions, and because it troubles them, they seek an escape from this reality.

Negating the norm

The second category of neutralisations where offenders deny their deviant actions is called *negating the norm*. Instead of distorting facts, perpetrators reject the norm relevant to the situation. They do this by *reducing norms to facts*, *appealing to another norm*, or *relativising the norm violation*. All three techniques were found to be relevant to ransomware crime.

Reducing norms to facts (Technique 4). Kaptein and Von Helvoort (2019) suggested that offenders may negate a norm by reducing it to facts (sub-technique 16: the reduction to facts) (Q: 2, 4, 19, 20, 22, 25, 28). One interviewee, for instance, stated that the world is built on financial gain and therefore there is no point in discussing whether ransomware is moral or not:

> The world is unfair to the weak, everything is built on financial gain. (Interviewee 1)

Kaptein and Von Helvoort (2019) argued that, in such scenarios, people simply assert that there are only facts, leaving no space for norms or normative judgements. Once facts are present, no interpretation of the situation is required. Maruna and Copes (2005: 227) noted that such neutralisations (e.g., 'i.e. just the way the world works') are more likely to be associated with persistent criminality. This has relevance in the context of ransomware since perpetrators commonly begin as hobbyists before engaging in minor cybercrimes, and eventually evolving into career criminals (Wall, 2021). Topalli (2006: 488) also found that offenders can argue that victimising is an unavoidable aspect of their life – 'It is just the fact'. Since the situation is out of their control, the offender can avoid feeling guilty.

Alternatively, individuals can reduce norms by using labels (sub-technique 18: the reduction to labels). Once a crime is re-labelled, it can then be denied, for example, referring to 'car theft' as 'joyride' (Copes, 2003), and stealing in the workplace as 'income adjusting' (Shigihara, 2013). Interviewee 5 referred to victims as 'business sharks' or 'capitalists', suggesting that it is acceptable for them to target (other) 'immoral' organisations (Q: 19, 20):

> We prefer to attack those who are like us – 'business sharks'. (Interviewee 5)

Essentially, the labels are likely used by the interviewee to distinguish between victims and 'normal' people or companies.

Another interviewee acknowledged wrongdoing but appeared to be apathetic to the societal norms and the opinions of others (sub-technique 17: the reduction to taste) (Q: 4).

Essentially, people acknowledge that there is morality (i.e., a set of norms) but it is subjective, which allows them to reject any form of accountability towards others and society at large. People commonly use these statements to justify deviant behaviour: 'It is my own life', and 'It is none of your business' (Kaptein and Von Helvoort, 2019: 1269). Eaton and Henry (1999) referred to this neutralisation as the claim of individuality, where people assert that they are unconcerned about the opinions of others regarding their behaviour.

When reducing norms to facts, interviewees also tend to blame another party by shifting the focus from their deviant inclinations to unethical propensities of potential victims (Interviewee 6) and justice system (Interviewee 5), which gives them the right to commit crime (sub-technique 19: the reduction to the immorality of accusers) (Q: 3, 20, 28).

Coined as *immorality of accusers*, using this sub-technique, offenders highlight misdeeds of others and therefore their 'right to criticise is denied' (Fritsche, 2002: 389). For instance, offenders accuse teachers of being unfair, victims (and potential victims) of conducting misdeeds, police of being corrupt, and even the whole justice system of being biased (Hinduja, 2007; Maruna and Copes, 2005; Stadler and Benson, 2012). Furthermore, Garrett et al. (1989) found that organisations that were accused of unethical practices defended their actions by referring to consumers who protested against

these practices as devious and malevolent. Subsequently, the norms advocated by accusers are dismissed. Sykes and Matza (1957: 668) labelled this technique as the *condemnation of condemners*, where individuals redirect the focus away from their own deviant behaviours towards the intentions and conduct of those who disapprove of their violations.

Alleged offenders also claim that a particular norm is invalid or irrelevant to them (sub-technique 20: the reduction to an invalid norm). Interviewee 6, for instance, used it to justify their involvement in ransomware activities (Q: 25).

In such instances, offenders actually acknowledge the existence of morality, but they assert their superiority above conventional norms. Kaptein and Von Helvoort (2019: 1269–1270) present the following examples: 'We are above the law', 'Rules are meant for other people' and 'Ethics and laws are for lesser firms'.

Appealing to another norm (Technique 5). When appealing to another norm, individuals acknowledge that the norm is violated, but they justify the violation by appealing to another more important norm (Q: 6, 7, 10, 11, 12, 20, 23, 24, 25, 28, 30, 31). Here, Interviewees 3, 4 and 5 (Q: 6, 11, 12, 24) were found to appeal to higher goals (sub-technique 21: the appeal to higher goals):

> 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. (Interviewee 3)

Schönbach (1990) referred to this technique as *the appeal to positive consequences*. Renfrow and Rollo (2014) explained that it is used by perpetrators to refute criminal acts by identifying valued consequences. Reported offenders asserted that these acts can benefit them and their families (Q: 11, 12, 24) as well as society at large (Q: 6). For instance, Renfrow and Rollo (2014) showed that individuals involved in sexting claimed that this activity helped them with their relationships. Similarly, Durkin and Bryant (1999) conducted content analysis of web forums used by paedophiles and found that offenders claimed that a sexual relationship with a child was beneficial to the child.

One interviewee explained that given the manner in which companies conduct business, it is unrealistic to anticipate outcomes different from what is currently happening to them (sub-technique 22: the appeal to others) (Q: 20, 28):

> There are cunning companies that do not want to spend money on protecting their network, pay salaries for good system administrators, and then [spend money] on ransom. (Interviewee 6)

Essentially, these offenders argue that the norm to be followed is determined by others – in this case by victims. If one does not invest in security, they cannot expect anything else but these attacks. In a sense, what others do (not do) is used for neutralisation. Prior literature referred to this technique as the *claim of normalcy* (Eaton and Henry, 1999).

Interviewees 3 and 5 appealed to their right to benefits (sub-technique 23: the appeal to rights) (Q: 7, 10, 23):

> We love our job. The money is not the target – the process is the important thing… The one of self-realisation. You should do the things that you can do the best because you need to realise your potential – this is a basic necessity for every human. (Interviewee 5)

Kaptein and Von Helvoort (2019: 1270) explained that when using this neutralisation technique, individuals 'hide behind moral and legal rights, by calling upon laws, rules, agreements, and promises'. For instance, Interviewee 5 claimed their right to self-realisation, while Interviewee 3 – to a right to proper material reward. Schönbach (1990) referred to this technique as the *right to self-fulfilment*. Fooks et al. (2013) found that corporate decision-makers go as far as referencing some unspecified universal right that protects the freedom of businesses to rationalise their deviant actions.

Similarly, quotes 7, 10, 23, 25, 30 demonstrated that alleged offenders (Interviewees 3, 5, 6 and 7) appeal to self-interest, arguing that it is reasonable to give priority to their own needs (sub-technique 25: the appeal to self-interest or lack thereof):

> There is one life and we take everything from it. (Interviewee 3)

Barriga and Gibbs (1996) referred to this phenomenon as *self-serving cognitive distortion* where one's personal opinions, expectations, needs, rights, immediate emotions and desires are important to a degree that the valid perspectives of others are hardly taken into account or disregarded completely. Essentially, people feel that they deserve benefits no matter the consequences for others (Gruber and Schlegelmilch, 2014). Coleman (1985) found that employees who steal from their employers sometimes deflect blame for their actions by rationalising that they deserve to reward themselves from time to time.

Findings also demonstrate that Interviewee 8 hides behind good intentions (sub-technique 24: the appeal to good intentions). In one particular instance, an interviewee explained that they typically reduce the amount of the demanded ransom – a gesture of goodwill or, in the words of Kaptein and Von Helvoort (2019), a good intention (Q: 31).

In these situations, people acknowledge wrongdoing, but the good motives render the behaviour not deviant. For instance, Ferraro and Johnson (1983) studied relationships between abusive husbands and their wives. Results demonstrated that certain high causes, for example, religious commitments, justify the abuse.

Relativising the norm (Technique 6). When offenders relativise a norm, they acknowledge that the norm was broken but mitigate the wrongfulness by comparing their actions with the actions of others. Essentially, individuals claim that their behaviour is not that bad (Kaptein and Von Helvoort, 2019).

Our findings suggest that reported ransomware offenders (Interviewees 3, 4, 5, 6, 8 and 9) use this neutralisation technique (Q: 8, 9, 16, 17, 18, 19, 21, 22, 26, 29, 31, 32). They claim, for example, that their aberrant actions are not as harmful as the actions of others (sub-technique 26: the relativisation by others). For instance, Interviewees 3, 4, 5, 6 and 9 shared that some ransomware gangs have no ethical considerations when they select their targets (Q: 8, 9, 16, 17, 18, 21, 26, 32):

> We have a negative attitude towards ransomware gangs that encrypt healthcare and educational institutions. (Interviewee 5)

> DarkSide was not completely without a moral compass. In a list of rules posted to the dashboard, the group said any attacks against educational, medical or government targets were forbidden. (*The New York Times*, Document 9)

Fritsche (2002) refers to this technique as the *sin of others*. Martin et al. (2014) found that employees used the *advantageous comparison* mechanism to justify some of their unethical behaviours by comparing them with even worse behaviours, making the original behaviour seem acceptable. Essentially, individuals claimed that 'it could be worse' (Martin et al., 2014: 303).

Interviewees 3, 4, 5, 6, 8 and 9 also claimed that the crimes they commit are not as serious as the crimes of others (sub-technique 28: the relativisation by seriousness). Attacking business sharks or capitalists appears to be 'less or not bad at all' (Kaptein and Von Helvoort, 2019: 1271) (Q: 8, 9, 16, 17, 18, 19, 21, 22, 26, 29, 31, 32).

> We are dealing with capitalists in the first place, which means they assess the risks, probable benefits, or losses from the deal. (Interviewee 5)

> Aleks states that he avoids targeting entities related to healthcare, labour unions and education. (Note: we were unable to verify such claims.) He criticised other ransomware offenders that do not share his ethical views, saying 'Just because you are a criminal, does not mean you have to stop being a human being. If you are attacking hospitals during COVID-19, you are a [expletive]'. (Cisco Talos, Document 4)

Liddick (2013: 624) referred to this neutralisation technique as *justification by comparison*, where people accept that they commit certain crimes but justify their acts by comparing them to more violent deeds: 'At least I am not out there killing people'. Cromwell and Thurman (2003: 546) noted that while these individuals may not be 'committed to conventional norms, they are nonetheless attempting to maintain their sense of self-worth by arguing that they could be worse or are not as bad as some others'. Researchers discovered that digital pirates (Hinduja, 2007) and individuals who illegally share files on peer-to-peer networks (Harris and Dumas, 2009) justify their behaviour by comparing it to more serious crimes, including, homicide, rape and marital violence.

Blaming the circumstances

The third category of neutralisation techniques, *blaming the circumstances*, describes instances where offenders accept that their behaviour is wrong, but reduce or completely deny responsibility for their actions by asserting that the circumstances are beyond their control. By externalising the blame, perpetrators free themselves from guilt when committing crimes. Our findings suggest that all three techniques are relevant to ransomware crime: they blame the *limited options*, their *limited role* and the *limited choice*.

Blaming the limited options (Technique 7). When blaming the limited options, offenders reduce or remove alternative options and subsequently claim that their actions are necessary due to the lack of 'real' options. Kaptein and Von Helvoort (2019) elaborate that people believe that it is unrealistic for them to behave well, given the circumstances. Some of the interviewees claimed to be confronted with unrealistic options (sub-technique 34: the limitation to unrealistic options), leading them to rationalise their non-conformities. For instance, Interviewee 1 stated that money is of central importance to this world. Since not everyone can earn money legitimately, they are left with no other realistic option, but to conduct crime (Q: 2). Similarly, Interviewees 3, 6 and 7 argued that sufficient revenue could not be obtained from legitimate work (Q: 10, 25, 30):

> This [pentesting] could not bring a proper material reward. (Interviewee 3)

Interviewees 2, 3 and 4 claimed that they are confronted with a unique option (sub-technique 35: the limitation to a unique option), viewing their particular situation as an emergency (Q: 5, 10, 13). They acknowledged that there was a legal option, but their unique circumstances justified them to follow a different path. Interviewees 2, 4 and 5 used excuses such as disability, medical emergency and inadequate cyber security industry in Russia to neutralise their behaviour (Q: 5, 13, 14, 24).

> It [the earnings from ransomware activities] gave me confidence for the future, and also the ability to pay for a very expensive surgery required for my brother. (Interviewee 5)

In summary, interviewees excuse their criminal activities by believing in the absolute inevitability of conducting ransomware crime. Morris and Higgins (2009) found digital pirates excuse their behaviour on the basis that, if one cannot afford software for work or studies, it is acceptable to download it illegally. Minor (1981) referred to this technique as a *defence of necessity* and argued that criminals who use it portray the criminal act as crucial to an individual's survival.

Blaming the limited role (Technique 8). In addition to blaming the limited options, offenders argue that they had a limited role in the crime. Accepting that there were other options, they can claim to have less or no relationship to the deviant behaviour, thus diminishing their responsibility (Kaptein and Von Helvoort, 2019). Interviewee 5, for instance, shifted the responsibility for the attacks to the victims (sub-technique 39: the limitation to others being responsible):

> Companies do not want to spend money on protecting a corporate network and hiring highly paid specialists. (Interviewee 5)

Interviewee 6 shared a similar sentiment (Q: 28).

Similar to the previous point, Interviewee 8 explained that a ransom price negotiation is possible but only to a certain extent. The interviewee underlined that if the victim insists on further concessions, they will break the initial deal and demand full payment. The victims will have no one to blame but themselves in this case:

Interviewer: Do you recommend any specific negotiators to the compromised businesses?

Interviewee 8: 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].

In studying youth anti-social behaviour, Barriga and Gibbs (1996) discovered that youth can deny their responsibility for anti-social behaviour by completely shifting responsibility to other parties. Bersoff (2001) found individuals tend to blame a company in order to reduce guilt. Similarly, our results suggest that ransomware offenders shift the responsibility for their wrongdoings to the victims.

Blaming the limited choice (Technique 9). People can also blame the circumstances by claiming to have limited choices. Offenders do not deny their moral autonomy but emphasise that this is threatened by pressures and temptations that are difficult to resist. Therefore it is reasonable that 'one succumbs to them' (Kaptein and Von Helvoort, 2019: 1275). Interviewee 1, for instance, explained that such an opportunity to earn is too big to miss, especially in a country where professionals with comparable skills are not in demand (sub-technique 44: the limitation to overwhelming temptation):

I am younger than you, but I have already earned for the rest of my life. Not millions, but enough to live in peace and never work. Here is a factor: how to quit a job that brings such earnings in a country where you are not much sought after? (Interviewee 1)

Kaptein and Von Helvoort (2019: 1276) elaborate that, in such instances, individuals refer to the existence of an irresistible opportunity, where one accepts that they have a choice to behave compliantly but choose not to; this choice is threatened by 'extreme demands on their personal integrity'. Interviewee 1 used the fact that people with their skills are not sought after in their country to justify their choice to act maliciously. Research confirms that some criminals go as far as blaming something or someone for pushing them to commit the crime. For instance, Vasquez and Vieraitis (2016) reported that one of their study participants, a street tagger, explained that walls call their names and tell them to tag. Sexual predators frequently use this argument and accuse their victims of being seductive and provocative and therefore impossible for the perpetrators to resist (Scully and Marolla, 1984).

Hiding behind oneself

When using the final three neutralisation techniques, offenders reduce or completely deny responsibility by hiding behind themselves or simply their own limitations. They suggest that they are not perfect human beings and do not have full control over themselves. Maruna and Copes (2005) elaborated that guilt can be mitigated through the capability to attribute bad behaviour to another part of the self that has been separated from the

real person. One can hide behind oneself by appealing to *imperfect knowledge*, *capabilities*, and *intentions* (Kaptein and Von Helvoort, 2019: 1275), and our results demonstrate that alleged ransomware offenders employ the last two.

Hiding behind imperfect capabilities (Technique 11). Individuals can claim that they are fundamentally uncontrollable and, therefore, do not possess the capabilities to resist bad choices. Schönbach (1990) refers to this technique as *impairment of capacity*. People claim that they do not have the power to stop themselves from conducting bad deeds. Interviewee 1 claimed their capacity impairment by explaining that it is not possible to reject an opportunity to earn so much money, while people with their skill set are in low demand (sub-technique 51: the hiding behind imperfect capabilities as a human being) (Q1).

Kaptein and Von Helvoort (2019) stressed that people who hide behind imperfect capabilities believe that all or most human beings have insufficient and inadequate capabilities and therefore cannot be held accountable for their wrongdoing. Rhodes and Cusick (2002) reported that women excused themselves for having unprotected sex due to their incapacity to negotiate. People can also claim that while they possess the capabilities to behave well, they do not have the ability to self-restrain in some situations (Taylor, 1972).

Upon data analysis, we found another quote that fell under Technique 11:

> I am against romanticising my work. Money is being stolen or extorted with my hands. But I am not ashamed of what I do. I sincerely try to find at least something bad in this and cannot. Probably my concepts of what is good and what is bad are somehow shifted. But in this case, they are shifted for many in this profession. (Interviewee 1)

Interviewee 1 is incapable of appreciating the societal norm. They know the norm but they (say that they) don't comprehend it. It was not clear to us if this relates to the technique 'Hiding behind imperfect capabilities'.

Hiding behind imperfect intentions (Technique 12). Finally, people can hide behind the lack of good intentions to excuse their behaviour. In such instances, individuals admit being ill-affected or unwilling to behave compliantly. Offenders understand what good behaviour is, but they are unwilling to act accordingly (sub-technique 57: the hiding behind imperfect preferences). For instance, Interviewee 7 is unwilling to take a white hat job as this would be a waste of their life:

> **Interviewer:** Do you have a white hat day job?
>
> **Interviewee 7:** To waste my life making a few dollars an hour?

Marshal (2017) explained that, when using this technique, individuals follow their desires and emotions despite the consequences – 'the heart wants what the heart wants'. Interviewee 7 unmistakeably puts high emphasis on their priority without considering the potential repercussions of ransomware attacks. Similarly, Interviewee 6 shared

that their primary focus is on achieving a higher quality of life, which they would not be able to afford on a salary. Accordingly, it is acceptable to continue with their trade:

> We are not planning to introduce restrictions [i.e., limit ransomware activities]. We only live once. Restrictions are created for people who want to live on a salary. (Interviewee 6)

Interviewees 6 and 7 engage in crime because they simply want to. Kaptein and Von Helvoort (2019) argued that this is the most unsafe neutralisation technique because an individual acknowledges that they misbehave willingly, which makes it close to confession. Copes (2003) interviewed 40 tow car thieves and discovered that they commonly use this neutralisation technique.

Discussion

To our knowledge, this study is the first to explore neutralisation techniques used by alleged ransomware offenders. The findings should be considered with the following limitations. The first one is the use of secondary data, and that the interviewees are potentially not representative of the wider group of ransomware actors, or that they were not genuine in their answers. Additionally, there is limited information on the reliability of transcripts (i.e., two documents mentioned light edits for clarity, see Table 1). We cannot be completely sure that no further edits took place or that the translation to English was perfect (Supplemental File A). The second limitation is the small dataset size ($n = 9$). Since we did not conduct interviews, we were also unable to reach saturation or observe a point of diminishing returns (Eisenhardt, 1989). The third limitation concerns the document search. It is possible that relevant publications were missed as a result of the keywords we adopted and/or the Google search algorithm (Papakyriakopoulos and Mboya, 2023; Wright, 2011). Search results were examined in the order of appearance until we reached a stage where the returns appear to have no relevance to our inquiry. The fourth limitation is linked to the model itself and our own ability to apply it. Kaptein and Von Helvoort (2019)'s model is very detailed and, while we found the paper helpful in understanding it, we did not reach a perfect agreement on all the quotes in the first instance. The fifth limitation is related to the validation of our results. On the topic of data validation in cybercrime community research, Hughes et al. (2024: 2) expertly pointed out that 'due to the adversarial and hidden nature of cybercrime, ground truth can be particularly difficult to establish'. One way to validate results is to use external data sources. For instance, certain underground forums are known to be criminals' hubs for knowledge exchange, communication, and trading of products and services. As such, analysing these forums enables researchers to better understand offenders' behaviour (Pastrana et al., 2018). Future studies should therefore focus on collecting data from underground forums to enrich current findings. A potentially promising avenue would be to ascertain if the neutralisation techniques ransomware offenders use differ between criminal groups or between members depending on their roles, for example.

Implications for research and theory

Although the interviewees tended to use neutralisations, the results suggest that most of them still commit to the dominant normative system (e.g., laws, values, norms, etc.) and therefore care about their self-image. Research shows that offenders often struggle with a negative perception of their identity (Durkin and Bryant, 1999) and therefore manage their self-image through cognitive manipulations. Our results demonstrate that some interviewees admit that their activities are destructive and even insist they are 'against romanticising their work'. However, they emphasise that these actions lead to positive outcomes, including driving the development of new technologies and educating companies about cyber security. Although admitting that they commit offences, some of the interviewees refer to themselves as 'human beings' who spare organisations such as hospitals, labour unions, educational establishments, etc. Such statements are potentially an attempt to influence public opinion about them or hackers more generally and change the negative perception of their identity. Rather than regarding themselves solely as 'criminals', some of the interviewees conceptualise themselves as 'criminals with good intentions'.

In this research, we used Kaptein and Von Helvoort (2019) model due to its comprehensiveness and granularity. In our previous research, we found six techniques relevant to ransomware, indicating that reported offenders invent facts about victims; blame victims for being attacked; appeal to higher goals, their rights and self-interest; and diminish the effects of crimes by comparing them to the actions of others (Connolly et al., 2023). All these excuses fall under the category of *denying deviant behaviour* in our current work. Our latest findings confirmed the previous results, but offered additional insights. Specifically, we learned that the interviewees tend to *deny responsibility* for the crimes they commit. They do so by (1) *blaming the circumstances*, including *limited options*, *limited roles* and *limited choices*, and (2) *hiding behind* their *imperfect capabilities* and *intentions* (i.e., *hiding behind oneself*). This is potentially very useful since a different type of intervention may be required for each of the four sub-categories in the model (Kaptein and Von Helvoort, 2019).

Next, our research suggests that ransomware offenders use at least nine neutralisation techniques to excuse their behaviour. We have not found any support for the three techniques in the model (i.e., *nuancing the fact* (T1), *denial of facts* (T2) and *hiding behind imperfect knowledge* (T10)). When using *nuancing the facts* technique, 'people escape reality by suggesting that there are no (hard) facts and that in general or in the specific situation there is no truth' (Kaptein and Von Helvoort, 2019: 1264). This is the safest way to excuse one's behaviour because offenders deny the truth and, if this technique fails, there are 11 more that can be used to reduce guilt. The fact that we could not find any evidence in support of the first technique is not surprising. First, the individuals who were interviewed had been selected because they were willing to talk about their involvement in ransomware attacks. Second, ransomware is a sophisticated type of crime that requires premeditation and sustained commitment. Similarly to computer hackers, ransomware actors do not outright reject their deviant actions but tend to provide excuses to rationalise their behaviour (Bossler, 2021).

The second technique, *denial of facts*, assumes that alleged offenders admit some validity to the situation, but they can still evade the complete truth by rejecting one or more

relevant facts. However, in order to conduct a valid analysis, the researcher must have all the facts relevant to the deviant behaviour. Several quotes (Q: 6, 8, 10, 15, 17, 18, 21), for example, could have been related to this technique, but, unfortunately, we lacked certainty regarding the accuracy of interviewees' statements about their reported criminal behaviour. For instance, Interviewee 3 claimed that they do not attack individuals, but it was impossible for us to confirm or refute it.

Kaptein and Von Helvoort (2019) explained that people selectively deny relevant facts, consciously pretending that nothing harm was inflicted. Von Hippel and Trivers (2011) argued that individuals engage in this self-deception by rehearsing lies in their minds until they depict a different truth. While we are unsure if the interviewees selectively denied facts, we found some evidence that they invented new facts about ransomware crimes they claimed to commit (Technique 3). This suggests that perpetrators might reduce guilt by distorting the facts about those.

We also did not find any evidence to support Technique 10. This discovery corroborates the notion that reported ransomware offenders, especially those interviewed, are not feigning ignorance about the deviant nature of their behaviour. Instead, they are conscious of the deviance inherent in their conduct. However, due to limited data we cannot confirm with confidence this finding.

Another interesting discovery is that interviewees tend to deny the wickedness of their actions (i.e., there is no problem at all because there is no deviant behaviour) more commonly than the responsibility (i.e., there is deviant behaviour but one is not responsible for it) (Kaptein and Von Helvoort, 2019). We made this inference because *denying deviant behaviour* category is supported by 39 quotes, while *denying responsibility* – by 16 (Supplemental File E). While this result is in agreement with Kaptein and Von Helvoort (2019) premise that it is safer for individuals to completely deny deviant behaviour (i.e., no crime was committed) than deny responsibility but, at the same time, admit the wrongdoing, it should be interpreted with caution due to limited data.

Conclusion

This article investigated neutralisation techniques used by studying individuals, who allegedly have taken part in ransomware criminal activities. Based on data from nine interviews, we found evidence of nine neutralisation techniques: denying wrongdoing through the invention of new facts or by negating societal norms. If the criminal behaviour could not be nullified, interviewees tended to deny responsibility by blaming the circumstances or their personal limitations.

The data used in this study makes this work unique and valuable for two reasons. Primary data on ransomware offenders is not easy to collect and secondary – not available in abundance in the public domain since these offenders are rarely arrested, tend to operate anonymously and rarely communicate about their activities. Furthermore, the data was collected from reported offenders who had not been apprehended. As such, the data is possibly more accurate and truthful than that collected from apprehended or convicted criminals whose accounts might be distorted by the prospect of a shorter prison sentence or more lenient treatment in prison (Pollock and Hashmall, 1991).

Acknowledgements

The authors would like to express sincere gratitude to Zayed University for providing Research Incentive Fund (Grant No. R22014) to conduct this research.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research project is funded by the Research Incentive Fund (Grant No. R22014) provided by Zayed University.

ORCID iDs

Lena Yuryna Connolly https://orcid.org/0000-0002-7110-9594
Hervé Borrion https://orcid.org/0000-0003-3624-4763

Supplemental material

Supplemental material for this article is available online.

References

Alwashali AAMA, Abd Rahman NA and Ismail N (2021, December) A survey of ransomware as a service (RaaS) and methods to mitigate the attack. In: 2021 14th International Conference on Developments in eSystems Engineering (DeSE), pp.92–96: IEEE.

Barriga AQ and Gibbs JC (1996) Measuring cognitive distortion in antisocial youth: Development and preliminary validation of the "how I think" questionnaire. *Aggressive Behavior* 22(5): 333–343.

Bersoff DM (2001) Why good people sometimes do bad things: Motivated reasoning and unethical behavior. *Personality and Social Psychology Bulletin* 25(1): 28–39.

Bossler AM (2021) Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice* 46(6): 911–934.

Brewer R, Fox S and Miller C (2020) Applying the techniques of neutralization to the study of cybercrime. In: *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. New York: Palgrave Macmillan, 547–565.

Cisco Talos Intelligence Group [CTIG] (2022) We keep your network safe, *Talos Intelligence*, available online: https://www.talosintelligence.com/about [Accessed September 2022].

Coleman JW (1985) *The Criminal Elite: The Sociology of White Collar Crime*. St. Martin's Press.

Connolly L, Borrion H, Arief B, et al. (2023) Applying neutralisation theory to better understand ransomware offenders. In: IEEE European Symposium on Security and Privacy, 5th Workshop on Attackers and Cyber-Crime Operations.

Connolly L, Wall DS, Lang M, et al. (2020) An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* 6(1): 1–18.

Copes H (2003) Societal attachments, offending frequency, and techniques of neutralization. *Deviant Behavior* 24(2): 101–127.

Cromwell P and Thurman Q (2003) The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behavior* 24(6): 535–550.

Dimitrievski I, Ridley A and Selck-Paulsson D (2023a) Levelling the field: The 'condemning the condemners' neutralization technique. *Orange Cyberdefense*, Blog, available online: https://

www.orangecyberdefense.com/global/blog/research/levelling-the-field-the-condemning-the-condemners-neutralization-technique.

Dimitrievski I, Ridley A and Selck-Paulsson D (2023b) We are not responsible for that – Neutralization through denials of responsibility. *Orange Cyberdefense*, Blog, available online: https://www.orangecyberdefense.com/global/blog/research/we-are-not-responsible-for-that-neutralization-through-denials-of-responsibility.

Durkin KF and Bryant CD (1999) Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant paedophiles. *Deviant Behavior* 20(2): 103–127.

Eaton R and Henry S (1999) *Degrees of Deviance: Student Accounts of Their Deviant Behavior*. Salem: Sheffield Publishing.

Eisenhardt KM (1989) Building theories from case study research. *The Academy of Management Review* 14(4): 532–550.

Europol (2023) Internet organised crime threat assessment. Report, Europol. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf.

Ferraro KJ and Johnson JM (1983) How women experience battering: The process of victimization. *Social Problems* 30(3): 325–339.

Flashpoint (2022) Who is Flashpoint? *Flashpoint*, available online: https://flashpoint.io/about-us/.

Fooks G, Gilmore A, Collin J, et al. (2013) The limits of corporate social responsibility: Techniques of neutralization, stakeholder management and political CSR. *Journal of Business Ethics* 112: 283–299.

Fritsche I (2002) Account strategies for the violation of social norms: Integration and extension of sociological and social psychological typologies. *Journal for the Theory of Social Behaviour* 32(4): 371–394.

Garrett DE, Bradford JL, Meyers RA, et al. (1989) Issues management and organizational accounts: An analysis of corporate responses to accusations of unethical business practices. *Journal of Business Ethics* 8: 507–520.

Gruber V and Schlegelmilch BB (2014) How techniques of neutralization legitimize norm-and attitude-inconsistent consumer behavior. *Journal of Business Ethics* 121: 29–45.

Harris LC and Dumas A (2009) Online consumer misbehaviour: An application of neutralization theory. *Marketing Theory* 9(4): 379–402.

Hinduja S (2007) Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology* 9(3): 187–204.

Hoevel GG, Veynshter A, Schutz F, et al. (2024) Will the ransom be paid? Examining influencing factors of the ransomware-payment decision. In: ECIS 2024.

Huang K, Siegel M and Madnick S (2019) Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys* 51(4): 1–36.

Hughes J, Pastrana S, Hutchings A, et al. (2024) The art of cybercrime community research. *ACM Computing Surveys* 56(6): 1–26.

Kaptein M and Van Helvoort M (2019) A model of neutralization techniques. *Deviant Behavior* 40(10): 1260–1285.

KELA Cyber Intelligence Center [KELA] (2022) About us, *KELA*, available online: https://ke-la.com/about-us/.

Lang M, Connolly L, Taylor P, et al. (2023) The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice*: 1–22.

Liddick D (2013) Techniques of neutralisation and animal rights activists. *Deviant Behavior* 34(8): 618–634.

Maimon D and Louderback ER (2019) Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology* 2: 191–216.

Marshal J (2017) Unethical rationalizations and misconceptions, *Ethics Alarm*, available online: https://ethicsalarms.com/rule-book/unethical-rationalizations-and-misconceptions/.

Martin SR, Kish-Gephart JJ and Detert JR (2014) Blind forces: Ethical infrastructures and moral disengagement in organizations. *Organizational Psychology Review* 4(4): 295–325.

Maruna S and Copes H (2005) What have we learned from five decades of neutralization research? *Crime and Justice* 32: 221–320.

Matthijsse SR, van 't Hoff-de Goede MS and Leukfeldt ER (2023) Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*: 1–27.

McGrath J (2021) Self-deception as a technique of neutralisation: An analysis of the subjective account of a white-collar criminal. *Crime, Law and Social Change* 75(5): 415–432.

Meland PH, Bayoumy YFF and Sindre G (2020) The Ransomware-as-a-Service economy within the darknet. *Computers & Security* 92: 1–9.

Meurs T, Junger M, Tews E, et al. (2022) How attacker's effort, victim characteristics and context influence ransom requested, payment, and financial loss. In: 2022 APWG Symposium on Electronic Crime Research (eCrime), pp.1–13: IEEE.

Minor WW (1981) Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime and Delinquency* 18(2): 295–318.

Morris RG and Higgins GE (2009) Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review* 34: 173–195.

O'Kane P, Sezer S and Carlin D (2018) Evolution of ransomware. *IET Networks* 7(5): 1–7.

Papakyriakopoulos O and Mboya AM (2023) Beyond algorithmic bias: A socio-computational interrogation of the google search by image algorithm. *Social Science Computer Review* 41(4): 1100–1125.

Pastrana S, Thomas DR, Hutchings A, et al. (2018, April) Crimebb: Enabling cybercrime research on underground forums at scale. In: Proceedings of the 2018 World Wide Web Conference, pp.1845–1854.

Pollock NL and Hashmall JM (1991) The excuses of child molesters. *Behavioral Sciences & The Law* 9(1): 53–59.

Popham JF and Volpe C (2018) 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* 12: 133–150.

Ransomware Task Force [RTF] (2022) A comprehensive framework for action: Key recommendations from the ransomware task force. *Institute for Security and Technology*.

Recorded Future (2022) Building the world's largest intelligence company, *Recorded Future*, available online: https://www.recordedfuture.com/our-story.

Renfrow DG and Rollo EA (2014) Sexting on campus: Minimizing perceived risks and neutralizing behaviors. *Deviant Behavior* 35(11): 903–920.

Rhodes T and Cusick L (2002) Accounting for unprotected sex: Stories of agency and acceptability. *Social Science & Medicine* 55(2): 211–226.

Ridley A and Selck-Paulsson D (2022) Noble vigilantes and victim-blaming: Neutralisation in cyber extortion by 'denying the victim'. *Orange Cyberdefense*, Blog, available online: https://www.orangecyberdefense.com/global/blog/research/noble-vigilantes-and-victim-blaming-neutralization-in-cyber-extortion-by-denying-the-victim.

Ridley A and Selck-Paulsson D (2023a) Reframing ransomware as a 'service' for the victim: The denial of injury neutralization technique. *Orange Cyberdefense*, Blog, available online: https://www.orangecyberdefense.com/global/blog/research/reframing-ransomware-as-a-service-for-the-victim-the-denial-of-injury-neutralization-technique.

Ridley A and Selck-Paulsson D (2023b) It might be wrong, but there was a good reason: Neutralization through an appeal to higher loyalties. *Orange Cyberdefense*, Blog, available online: https://www.orangecyberdefense.com/global/blog/research/neutralization-through-an-appeal-to-higher-loyalties.

Russian OSINT (2022) Description, *Russian OSINT*, available online: https://www.youtube.com/c/RussianOSINT/about.

Schönbach P (1990) *Account Episodes: The Management or Escalation of Conflict*. Cambridge: Cambridge University Press.

Scully D and Marolla J (1984) Convicted rapists' vocabulary of motive: Excuses and justifications. *Social Problems* 31(5): 530–544.

Selck-Paulsson D and Ridley A (2022) Do ransomware and cyber extortion threat actors know deep down that their activities are criminal or deviant? *Orange Cyberdefense*, Blog, available online: https://www.orangecyberdefense.com/global/blog/do-ransomware-threat-actors-know-that-their-activities-are-criminal.

Shigihara AM (2013) It's only stealing a little a lot: Techniques of neutralization for theft among restaurant workers. *Deviant Behavior* 34(6): 494–512.

Stadler WA and Benson ML (2012) Revisiting the guilty mind: The neutralization of white-collar crime. *Criminal Justice Review* 37(4): 494–511.

Sykes GM and Matza D (1957) Techniques of neutralization: A theory of delinquency. *American Sociological Review* 22: 664–670.

Taylor L (1972) The significance and interpretation of replies to motivational questions: The case of sex offenders. *Sociology* 6(1): 23–39.

The New York Times [TNYT] (2022) Company, *TNYT*, available online: https://www.nytco.com/company/.

Topalli V (2006) The seductive nature of autotelic crime: How neutralization theory serves as a boundary condition for understanding hardcore street offending. *Sociological Inquiry* 76(4): 475–501.

Vasquez A and Vieraitis LM (2016) "It's just paint": Street taggers' use of neutralization techniques. *Deviant Behavior* 37(10): 1179–1195.

Von Essen E, Hansen HP, Nordström Källström H, et al. (2014) Deconstructing the poaching phenomenon: A review of typologies for understanding illegal hunting. *British Journal of Criminology* 54(4): 632–651.

Von Hippel W and Trivers R (2011) The evolution and psychology of self-deception. *Behavioral and Brain Sciences* 34(1): 1–16.

Wall D (2021) 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: 1–11.

Wright JD (2011) Defining and measuring search bias: Some preliminary evidence. *International Center for Law & Economics*, November, pp.12–14.