Article

Police Journal: Theory, Practice and Principles

The Police Journal:
Theory, Practice and Principles
2023, Vol. 96(4) 573–592

DOI: 10.1177/0032258X221107584
journals.sagepub.com/home/pjx

Understanding cybercrime in 'real world' policing and law enforcement

Joanna Curtis
School of Computing, Newcastle University, UK

Gavin Oxburgh
Department of Social Sciences, Northumbria University, UK

Abstract
Cybercrime is a growing issue, still not fully understood by researchers or policing/law enforcement communities. UK Government reports assert that victims of cybercrime were unlikely to report crimes immediately due to the perception that police were ill-equipped to deal with these offences. Additionally, these reports identify policing issues including a lack of cybercrime knowledge. This paper reviews current research, providing a comprehensive account of cybercrime and addressing issues in policing such offences. We achieve this by describing the technological, individual, social and situational landscapes conducive to cybercrime, and how this knowledge may inform strategies to overcome current issues in investigations.

Keywords
Cybercrime, crime, cyber-criminals, policing, strategies, investigations

The 'cyber' in cybercrime

Although it is universally agreed that cybercrime exists, there is no universal definition of what it means (Holt and Bossler, 2014; Kshetri, 2010; Wall, 2017a). Terms including cybercrime, cyber-crime, computer crime, cloud-crime and computer misuse are often used interchangeably and can refer to any internet- or computer-related criminal activity (Goodman and Brenner, 2002). Throughout this paper, any criminal behaviour utilising the Internet will be termed 'cybercrime' unless referring to specific research using other

Corresponding author:
Joanna Curtis, School of Computing, Newcastle University, Newcastle upon Tyne, NE1 7RU, UK.
Email: joanna.curtis@newcastle.ac.uk

terminology. Whilst recognising that cybercrime is a global issue, this paper will focus primarily on policing cybercrime in England and Wales.

It is widely accepted that cybercrime is highly prevalent and increasing. A recent report suggests that Internet Service Providers (ISPs) record around 80 billion automated scans daily by online perpetrators with the aim of identifying targets for cybercrime (Lewis, 2018), and in the year ending September 2019, 1 million 'computer misuse' crimes were reportedly committed against households in England and Wales (National Crime Agency [NCA], 2020). Online crime is growing not only in incidence but also as a percentage of all crimes. The Crime Survey for England and Wales reports an increasing proportion of recorded crimes being 'flagged' by police as online crime, with anecdotal evidence suggesting that such 'flags' remain under-used (Office for National Statistics [ONS], 2017, 2018, 2019a).

Whereas traditional crimes are decreasing in Western countries, cybercrimes are increasing beyond this rate of reduction (Caneppele and Aebi, 2019). It has also been noted that decreases in traditional crime predate the emergence and growth of cybercrime (Farrell et al., 2015). This, combined with differing offence and offender characteristics, means it cannot be assumed that the rise of cybercrime caused the downturn in offline crime, nor that those offenders traditionally acting offline are now turning their hand to cybercrime instead (Farrell et al., 2015). Whatever the cause, crime is now evolving and growing into the online realm, intensifying the downward trajectory of traditional crime incidence (Caneppele and Aebi, 2019).

This increase in, and shift to, cybercrime, combined with interchangeable and often confusing terminology, has led to recent suggestion that the prefix 'cyber-' may soon become redundant, as almost all crimes will be touched by technology (Furnell and Dowling, 2019). Indeed, all serious and organised crimes investigated now feature some encryption, and the Internet is used in the recruitment, victimisation and profiteering, of traditionally offline crimes such as counterfeiting physical currency (NCA, 2020).

The role of the internet

Since becoming widely available several decades ago, the Internet has facilitated offences to varying degrees, typified by Wall (2007) as cyber-assisted, cyber-enabled and cyber-dependent crimes. Kirwan and Power's (2013) typology similarly features internet-enabled (i.e. cyber-enabled), internet-specific (i.e. cyber-dependent) crimes and crimes against the virtual person. The two concepts common between typologies appear robust – current National Cyber Security Strategy (HM Government, 2016) recognises only cyber-enabled and cyber-dependent crimes, and that these two types are interrelated. Cyber-enabled crimes are defined as traditional crimes which are increased by scale or reach by technology (e.g. fraud), while cyber-dependent crimes are offences that would be impossible in the absence of the Internet (e.g. ransomware; HM Government, 2016; NCA, 2020). While these crimes may be related to offline offences such as theft, burglary, criminal damage or fraud, cybercrimes are not synonymous with their offline counterparts, and are experienced differently by victims, perpetrators and authorities (see Bocij and McFarlane, 2003; Leukfeldt and Yar, 2016; ONS, 2020; Zhang et al., 2007).

Exponential growth in worldwide Internet use is associated with increased numbers of offences using the Internet and the 'cloud' (Holt and Bossler, 2014), as they provide an increased, centralised, pool of victims and new opportunities to both commit crime and to evade detection and prosecution (Kshreti, 2010; Reep-van Den Bergh and Junger, 2018; Wall, 2017b). The increased use of social media technologies has meant that a single offender can now reach a greater number of victims (see Wall, 2013) and both the costs and skill-levels required to commit cybercrimes have decreased (Sood and Enbody, 2013; Wall, 2017a). Online communities offer ready-made packages of malicious software (i.e. malware) that can be sold to unskilled individuals, and instructional material is freely available, admitting average internet users to the world of cybercrime (Denning, 2011; Holt, 2009; Jordan and Taylor, 2004; NCA, 2020). It is, therefore, becoming easier, cheaper and more convenient for people to commit cybercrime and on a larger scale.

This change has been exacerbated by developments in cloud technology (Wall, 2017b) bringing increased computer storage and processing power. By providing an online pool of shared resources, facilitating access to 'off the shelf' attack software and processing resources such as botnets to perform and automate attacks (Mell and Grance, 2009; Wall, 2017b), the cloud presents an online environment in which offenders can hunt, operate and distribute spoils with relative ease and anonymity. By its very nature as a shared data centre, cloud technology increases the number of devices that can be accessed through an Internet connection and thus the number of opportunities for offenders to exploit (Wall, 2017b). The effect of the cloud as a force multiplier not only results in a greater yield to perpetrator efforts but also further reduces the risk of prosecution. Thus, the Internet and cloud computing offer a spectrum of criminal options, from the influence of a networked computer on traditional crime, to crimes that are automated and occur entirely within a virtual environment.

Human elements of cybercrime

Human users often represent the weakest link in computer security and, depending on the type of cybercrime, their weaknesses can be exploited in various ways – making victims instruments of their own victimisation. Means of exploitation include social engineering and trickery, manipulation of decision-making processes through perceived urgency or authority and utilisation of predictable habits relating to website use, downloads, password use and social or professional networking (Nurse, 2019). Victims may, therefore, blame themselves or experience blame from others, in addition to potentially devastating consequences such as financial loss or damage to reputation and career (Button, 2020). Most victims of cybercrime report being affected emotionally, ranging from annoyance to depression, insomnia, anxiety and panic attacks (ONS, 2020). Each year, a higher percentage of cyber fraud victims report emotional effects than non-cyber fraud victims (ONS, 2020). Victims of cybercrime can suffer lasting psychological and emotional effects including Post-Traumatic Stress Disorder (PTSD), with associated impacts on physical health (Button et al., 2020; Cross et al., 2016; Jansen and Leukfeldt, 2018; Kirwan and Power, 2013). Victims may also feel ashamed or violated by an invasion of their privacy or experience the breakdown of relationships following financial

loss, leaked information, sextortion[1] or romance scams (Cross et al., 2016; Nurse, 2019). Most seriously, there are potential physical risks amounting to danger to life due to meeting strangers in real-life or attacks on vital services such as power and healthcare (Cross et al., 2016; Bada and Nurse, 2020; Nurse 2019). Online sexual exploitation and human trafficking are other examples of high-impact crimes which have been facilitated and increased through the Internet, as perpetrators can more easily access victims and recruit fellow offenders, distribute materials anonymously and access a far greater number of potential customers, driving demand for these offences to be committed. As with many other forms of serious and organised crimes, the dark web enables much of this offending to continue despite law enforcement efforts (NCA, 2020).

Whilst most internet users report fear of cybercrime, the importance of information security and concerns over privacy, only a minority of users translate these into preventative behaviours, even following victimisation (Button et al., 2020). This discrepancy between privacy attitudes and behaviours is known as the 'privacy paradox' (Barnes, 2006; Gerber et al., 2018). Proposed to stem from a false sense of computer security and over-reliance on software, engaging security measures could even *increase* the risk of victimisation (Holt and Bossler, 2013; Reyns, 2015; Reyns et al., 2016). The findings of Jansen and Leukfeldt (2016) demonstrate this, as most phishing victims had security software but admitted having negligently given out security codes to perpetrators. Even when individuals had an awareness of security cues on websites (e.g. broken images or unusual URLs), this often failed to translate into caution (Downs et al., 2006). The online disinhibition effect (Suler, 2004) helps explain this phenomenon; referring to the way in which Internet users seem to self-disclose more information online than they would offline, sometimes attributed to dissociation from the real-world and perceptions of anonymity and invisibility. This tendency to over-share online can cause personal information to become easily available to potential cyber-criminals (Nurse, 2019).

This dissociative anonymity and resultant discrepancy between offline and online behaviours (termed as 'toxic disinhibition'; Suler, 2004) extend to increased online antisocial behaviour, deviancy, crime and violence. Compared with traditional crime, cybercrime offers a greater degree of protective anonymity with many ways for an attacker to disguise their identity online, even assuming a new persona (e.g. Nurse, 2019; Richie and Freiburger, 2014). This separation of identities means that individuals do not experience behavioural inhibitions to the same extent as in off-line contexts (Hinduja & Patchin, 2008; Slonje and Smith, 2008), partly from a decreased sense of proximity to the victim, producing reduced feelings of guilt and fear of retaliation (e.g. Bocij and McFarlane, 2003; Schaefer, 2014). Cyber-criminals also perceive the risks of being caught by authorities as relatively low, and any consequent sanctions minor, presenting little deterrent from this type of crime (Zhang et al., 2007). The lack of adequate deterrence combines with motivating factors, described later, to encourage individuals into cybercrime.

Who commits cybercrimes?

Having established why the internet provides an almost optimal criminal environment, our attention turns to cybercriminals themselves. The literature suggests that cybercriminals, notably hackers, are not a homogenous group as previously thought (Furnell, 2010). An increasing number of offender typologies, developing in complexity as the crimes and perpetrators appear to, feature differing motivations, personality traits, methods and capabilities (e.g. Furnell, 2010; Gaia et al., 2020; Moeckel, 2019; Seebruck, 2015). Due to the anonymous nature of cybercriminals, these typologies are difficult to validate, often relying on data from offenders who are caught, representing the minority.

The known demographic characteristics of cyber-criminals differ from those of traditional offenders in some ways. For example, education and employment are typically significantly associated with reduced risk of traditional offending, but no significant equivalent relationships exist regarding cybercrime (e.g. Bonta and Andrews, 2017; Weulen Kranenbarg et al., 2018). However, employment and education specifically relating to Information Technology may be linked to increased risk of cybercrime perpetration (Weulen Kranenbarg et al., 2018). The established relationship between household composition and offence perpetration (Bonta and Andrews, 2017) is present and more pronounced in cybercrime, despite expectations that crimes committed on a computer would be relatively unaffected by the presence of others in the home (Weulen Kranenbarg et al., 2018).

The literature suggests that hackers are likely to start whilst they are young, with 61% starting between the ages of 10 and 15 years, and another 32% starting between 16 and 20 years old (Chiesa et al., 2008). In fact, the average age of suspects in UK National Cyber Crime Unit investigations in 2015 was 17 years old (NCA, 2017). However, hackers range considerably in age and regularly defy this stereotype (e.g. see Steinmetz, 2016). Additionally, research findings imply that the typical hacker is, '…racially white, masculine-gendered and… decidedly middle class' (Steinmetz, 2016: p. 36). This extends to cybercriminals in general, as Harbinson and Selzer (2019) found that convicted cyber-dependent crime offenders tended to be white and male but an average age of 38.2, a far cry from the teenaged hacker stereotype. It has, however, been suggested that the severity of cybercrimes (and thus the likelihood of conviction and inclusion in such research) increases with offender age (Hutchings, 2014). This is consistent with findings from the UK's National Crime Agency (NCA) who, in partnership with CREST (the Council for Registered Ethical Security Testers)[2], propose a pathway from computer games, to online games, gaming cheats, gaming modifications, hacking forums, to cybercrime of escalating severity (CREST, 2015; NCA, 2017).

Why commit cybercrime?

In the pathway to cybercrime, gaming modification represents an important step – crossing boundaries of law to achieve antisocial and financial goals, reflecting cybercrime itself (Curtis and Oxburgh, 2021). Gaming modifications and cybercrime also share a strong community aspect, centred around the use of forums for participants to socialise,

share ideas and work collaboratively and/or competitively; these communities are considered important in the progression to cybercrime (NCA, 2017). Hackers and other cybercriminals develop relationships and networks, both on- and off-line (Leukfeldt et al., 2017) with hacking communities providing 'guild-like social and learning structures' (Steinmetz, 2015: p130). The hacking culture places a strong emphasis on abilities and skills which dictate social standing within these communities – encouraging the acquisition of knowledge and pursuit of challenge, and rewarding success with status (Steinmetz, 2015).

Social motivations to offend. Whilst the literature suggests that intellectual challenge and curiosity are the strongest motivator for hacking security systems, this was not found to correlate with actual hacking frequency, casting doubts on the reliability of self-reports; proposed to reflect culturally recognised motivations, rather than true personal motivations (Madarie, 2017). The second strongest motivator indicated by the literature, peer recognition and respect, *was* found to be correlated with hacking – the more highly motivated by recognition and respect from peers, the more often a hacker attempted to circumvent security systems (Madarie, 2017).

Holt et al. (2020) found that hacking for website defacement was primarily motivated by the high-visibility of the target, supporting other findings that the pursuance of status and reputation within the hacking subculture is a strong motivator, as these are afforded by attacks on high-visibility targets (Steinmetz, 2016). Hacking website homepages was found to be motivated by ideology or a sense of challenge, whereas secondary pages were hacked for fun, to be the best, be patriotic or for no particular reason (Holt et al., 2020). These offenders tend to be proud of their crimes, wanting others to know they were responsible (Woo et al., 2004), possibly because recognition opens the door to better online groups and hacking sites, bringing greater resources and prestige (Goode and Cruise, 2006).

Other motivations to offend. Some research studies suggest that offenders become involved in cybercrime due to the promise of financial gain (Hutchings, 2014), and monetary reward has been found to be one of the most important motivations for perpetration of virtual theft and online identity fraud (Kerstens and Jansen, 2016). However, some research studies find money to be the least motivating factor to hackers (Madarie, 2017) and software crackers (Goode and Cruise, 2006).

Fun and entertainment have also been found to be an important factor in the motivation to commit identity fraud and hacking crimes (Kerstens and Jansen, 2016; Turgeman-Goldschmidt, 2005). Reasons for perpetration include hackers beating the system as a 'prank' (Woo et al., 2004), team-play and intellectual challenge (Madarie, 2017). Some perpetrators have stated that the harder the hacking was, the more enjoyable the experience (Goode and Cruise, 2006). Conversely, some researchers have suggested that ease and lack of deterrence are motivation for hacking (Turgeman-Goldschmidt, 2005).

Forum communities

Much of the research providing insight into the above motivations was performed using online forums, a source of information common in relevant literature. Hacking forums generally allow hackers to 'belong' to an extensive social network and identify with a larger hacking community (Woo et al., 2004). In addition to recruiting through social contacts in the offline world, forums help individuals to find suitable co-offenders and play a role in the formation and growth of many cybercrime networks (Leukfeldt et al., 2017; Nurse & Bada, 2019). This is may be due to the combination of malicious and benign content on forums. Users who are initially interested in computer gaming or technology may find the hacking or fraudulent activities to which they are exposed alluring, for the sake of curiosity and challenge, and to improve both their finances and reputation within the community (Goldsmith and Wall, 2019; Pastrana et al., 2018). Current literature highlights the importance of trust, status and respect in these forum communities, and illustrates how such forums can be used to aid learning in young perpetrators, as proposed by National Crime Agency reports (CREST, 2015; NCA, 2017).

Cybercrime forum users are assigned to groups which correspond to their social status on the site (Motoyama et al., 2011). For example, online black markets, mostly trading in malicious tools, featured hierarchies ranging from introductory membership levels, such as newbie and newcomer, to higher-status ranks of moderator or administrator (Radianti, 2010). Learning and knowledge appear to be central to this status level in hacker subculture, and the quality of information or creative use of materials by users could increase their status level (Holt, 2007).

Research has suggested that forums do not only reflect users' abilities but are actively used by many individuals to learn and teach others about how to hack and commit online fraud, and there is evidence this starts at a young age (Hutchings, 2014). One offender interviewed by Hutchings (2014) reported that he had initiated up to 40 other people by teaching them to hack on online forums and had communicated with over 200 others. This application of online forums is supported by the values demonstrated by their content; that continued study, practice and significant effort are required to be good at hacking (Holt, 2007). Similarly, forum users are ridiculed and attacked when they show ignorance or inexperience (Radianti, 2010). Combining the social desirability of successful and sophisticated hacking skills, and the shaming of those deemed to lack them, generates an environment strongly promoting the acquisition and improvement of these abilities.

Hacking forums consequently tend to provide tools used to teach users basic hacking knowledge, malware creation, phishing and Facebook hacking tutorials and general programming (Samtani et al., 2015). These tutorials have been linked to increases in cybercrime perpetration, as those who have learnt about computer activity from such forums have been found to be more likely to engage in hacking behaviours and the creation of malware (Skinner & Fream, 1997).

Combining factors

Not all gamers, internet and forum users commit cybercrime, nor do cybercriminals use the internet exclusively for criminal activity. The crossing of boundaries between benign and criminal online behaviours, particularly in younger individuals, is referred to as 'digital drift' (Goldsmith and Brewer, 2015) and stems from Matza's (1964) concept of a 'drift' in and out of criminality exhibited in juvenile delinquency. Matza argued that, '…the delinquent transiently exists in a limbo between convention and crime … he drifts between criminal and conventional action' (p.28). Matza describes the importance of subcultures, a loosening of binds to law and morality and a neutralisation of crime through a perception that the victim, the crime or the authority policing it are in some way invalid or inapplicable (see also Sykes and Matza, 1957). Applying this concept to cybercrime, substantiated by recent research, Goldsmith and Brewer (2015) concluded that peer association with those who support cyber-offending significantly increases cybercrime perpetration, even more than pre-existing computer knowledge (Nodeland and Morris, 2020).

The peer association, dissociative anonymity, mobility and distance from the offline world, described previously in this paper, aid our understanding of the Internet's role in providing not just an environment littered with criminal opportunities but the 'moral vacuum' Matza (1964, p.181) considered conducive to offending when combined with will to engage these opportunities.

The Investigation of Cybercrime: Current Issues in Policing

Cybercrime has proved notoriously difficult to investigate and successfully prosecute (e.g. NCA, 2020; Yar and Steinmetz, 2019). A multitude of issues in policing cybercrime influence this difficulty, which is broadly categorised into two areas: (i) establishing the responsibility of the police to investigate and (ii) conducting the investigation.

Establishing police responsibility

In order for the police to investigate an incident, they must first become aware that it has occurred, but research suggests that victims of cybercrime are less likely than those of traditional crime to report their victimisation to the police or other authorities (Van de Weijer et al., 2019). This is supported in national statistics, as the 'dark figure' of cybercrime (the disparity between estimated and reported crime incidence) is greater than that of traditional crime. For example, as compared with 54.5% of victims of theft offences[3], only 15.3% of estimated total victims of fraud and computer misuse report these crimes to the police or other relevant authorities[4] (ONS, 2019b). In addition to perceptions of police being unprepared for cybercrime (HMIC, 2015), reasons for victim non-reporting of cybercrimes include not knowing that the act was classed as a criminal offence, not having heard of Action Fraud or realising that they addressed cybercrime, believing that the police or Action Fraud were unlikely to act on a report, and preferring to deal with the matter themselves (Button et al., 2020).

Police contend with additional legal and practical difficulties in identifying cybercrime. As legislation attempts to keep up with emerging technology and the rapid

evolution of crime, investigators often find themselves in unknown territories of the law; specifically, if it is currently illegal and a matter for the police (Criminal Law Reform Now Network [CLRNN], 2020). Many victims feel their victimhood is not fully recognised and acknowledged by police, some are even mistakenly informed outright that they are not victims of a criminal offence, leaving them feeling ignored, embarrassed and without justice (Button et al., 2020; Leukfeldt et al., 2020).

Jurisdictional issues surround geographical locations of victims, suspects, the technology used and thus, where the crime occurred (CLRNN, 2020; HMIC, 2015; Holt and Bossler, 2015). Assuming criminal offence and location are established, both victims and police report uncertainty over whose role it is to investigate; responsibility may be deemed to lie with the police, Action Fraud (in England, Wales and Northern Ireland), National Fraud Investigation Bureau (NFIB), National Crime Agency (NCA), ISPs, websites, financial institutions or insurers (HMIC, 2015; Holt et al., 2015). Demonstrating the lack of clarity, a single paragraph in a government publication directs readers seeking advice to the National Cyber Security Centre's website, but instructs readers to report cybercrime to Action Fraud, the police or Crimestoppers (NCA, 2020).

Action Fraud (run by the City of London Police) is the UK's national reporting centre for fraud and cybercrime (Action Fraud, 2020a) who takes reports from victims, then pass the information onto the NFIB for analysis and potential investigation by a local police force if there is deemed to be a realistic probability of identifying a suspect (Action Fraud, 2020a; HMIC, 2015). Victims of cybercrime have reported confusion over the Action Fraud and police websites regarding what should be reported and to whom, misconceptions that Action Fraud is manned by members of a police fraud squad, and that Action Fraud are the incorrect reporting body for non-fraud cybercrimes because of the name 'Action Fraud' (Button et al., 2020). Recent statistics show that 65% of victims of offline fraud are satisfied with Action Fraud handling, compared with only 46% of cyber fraud victims, who outnumber offline fraud victims 3:2 (ONS, 2020). Further, 50% of cyber fraud victims are unsatisfied in a statistically significant increase from 2 years prior (ONS, 2020).

The remit of Action Fraud is unclear to victims, not only because of the name (Button et al., 2020) but also the website itself. For example, 'medical scams' appear on conflicting Action Fraud pages stating that these crimes both *cannot* and *should* be reported to them (Action Fraud, 2020a, 2020b). Confusing things further, whilst Action Fraud refers to themselves as the UK centre for reporting, they have no remit in Scotland, where police hold this responsibility. The lack of a transparent and straightforward process for identifying, reporting and investigating cybercrimes leaves both victims and police investigators confused (Button et al., 2020; HMIC, 2015; HMICFRS, 2019).

Conducting the investigation. Most of the lower ranking police officers surveyed in England and Wales believe cybercrime is a serious problem in society, and that members of the public or local community do not truly recognise the risks and threats it presents (Holt et al., 2019; Lee et al., 2019). However, victims consider police ill-equipped to deal with cybercrime (HMIC, 2015), and research has supported this assertion with 61% of officers categorised as 'unprepared' to respond to cybercrime (Burruss et al., 2019). Policing/law

enforcement agencies have been found to lack knowledge about crime on the Internet (Hadlington et al., 2018; Jewkes and Leukfeldt, 2012), and the lack of understanding in law enforcement is considered a highly influential factor in low cybercrime conviction rates (see Dubord, 2008; Leibolt, 2010).

Many police officers perceive cybercrime as unique and distinct from traditional crimes, rather than as an extension or adaptation of them (Holt et al., 2019). Perceived differences between cybercrimes and traditional crimes, and thus perceived applicability of existing skills and experience, reportedly affect investigators' sense of preparedness and confidence in responding to cases of cybercrime (Bossler et al., 2019). Better understanding and appropriate training are considered crucial in the response to cybercrime (HMIC, 2015). Indeed, officer training was found to be a key determinant in perceived preparedness to deal with cybercrime cases, and training was also found to predict an officer's preparedness to engage with victims (Burruss et al., 2019).

Initial investigations consist of obtaining accounts from victims and witnesses, ensuring their needs are met, identifying suspects, examining crime scenes, identifying further potential sources of evidence and documenting and submitting all relevant records and intelligence gathered (College of Policing, 2020). In cybercrime investigations, this process is not only impeded by the lack of knowledge regarding cybercrime but also the anonymity of suspects (and often victims), lack of investigator understanding of these individuals and their lives and the asynchronous and non-physical nature of the Internet itself.

The anonymous nature of the Internet presents practical difficulties for investigating officers, as it is difficult for frontline officers to identify unknown individuals based on a virtual footprint (Dodge and Burruss, 2019). Consequently, investigators cannot obtain accounts from victims or witnesses, meet their needs, identify potential sources of evidence (e.g. personal computers) and otherwise progress the investigation (College of Policing, 2020). A literature review conducted by the current authors finds that reliable risk factors for victimisation are yet to be established. Victims often appear to perpetrators simply as a series of numbers – this makes protecting the public, identifying and managing the needs of victims and preventing future victimisation problematic.

When identified, government-commissioned reports (e.g. Button et al., 2020; HMIC, 2015) found that investigating officers did not respond to victims effectively. This included not taking evidence collected by the victim; failing to provide adequate support, advice and updates; and generally exhibiting a lack of understanding about the threat and risk to the victim (and others). Police report difficulties understanding those who lead online lives, resulting in problems during suspect and victim interviews (HMIC, 2015). The lack of understanding of the social and technical elements of cybercrime inhibits an investigator's ability to empathise which, in turn, impacts the success of an investigation (HMIC, 2015). Simply put, if officers do not understand the world that cybercrime victims and offenders inhabit, they are unlikely to understand the individuals and their needs.

The role of empathy in investigations

The role of empathy in investigations, specifically during interviews, has support in the research literature. Empathy from police interviewers has been associated with both increased suspect cooperation (Holmberg and Christianson, 2002) and reduced victim attrition and PTSD (Maddox et al., 2011) in cases of sexual offences. Government reports suggest that whilst police may find it difficult to empathise with victims (and suspects) of cybercrime, the majority of victims who contact Action Fraud or the police are satisfied with the reporting process and advice given (Button et al., 2020; HMIC, 2015; HMICFRS, 2019).

Empathy is associated specifically with suspect cooperation and considered to be vital at interview (Holmberg and Christianson, 2002; Oxburgh and Ost, 2011; Oxburgh et al., 2014), but suspects of cybercrime are reportedly somewhat of an unknown entity to police, perhaps because of the great diversity in both cyber-dependent crimes and cybercriminals themselves (HMIC, 2015; HMICFRS, 2019; Seebruck, 2015). Consequently, establishing common ground at interview can be difficult, and there are some stereotypes of cyber-criminals that may even be counterproductive as they often do not hold true (Steinmetz, 2016). The impact of empathy in interviews specific to cybercrime has yet to be established with empirical evidence, despite reports that a lack of empathy impacts police decision-making in such investigations (HMIC, 2015).

A further practical issue for investigators is that cybercrime attacks can be operationalised and distributed in advance indefinitely, making it even harder for investigators to establish a timeline (Dodge and Burruss, 2019). Victims who do report cybercrimes to the police often delay their reporting due to embarrassment or a perception that they are better equipped or motivated to rectify the situation than the police are, putting even more time between the act and any possible evidence collection (HMIC, 2015).

With remote and asynchronous offending by means not understood and persons unknown, lead generation becomes problematic, alibis cannot be relied upon and police have reported confusion as to the collection of evidence, leaving some with victims who feel dismissed (HMIC, 2015). Insufficient expertise in frontline officers and their identification, collection and processing of evidence is a recognised issue in the response to cybercrime (Dodge and Burruss, 2019). When evidence is collected, digital forensics routinely experience backlogs of up to a year or more, time that a victim is without their device, doing little to encourage the pursuance of charges (HMIC, 2015; Mayor of London, 2019).

Thus, it seems reasonable that the public reportedly believe that the police do not take cybercrime, or its victims, seriously (HMIC, 2015; United Nations Office on Drugs and Crime, 2013) and lack the ability to properly investigate 'high-tech' offending (Brown, 2015). The result is a vicious cycle in which, due to a lack of faith in police effectiveness, victims fail to inform the police, who are consequently unable to respond in an effective way (Brown, 2015). This ineffective and inconsistent response presents inadequate deterrence and even greater motivation for cyber-criminals which, in turn, leads to further offending (Holt et al., 2019; Wall, 2017a).

Implications for practice

Legal and practical issues in the investigation and prosecution of cybercrime incidents may be somewhat mitigated by equipping officers with improved understanding of the procedural, technical and personal elements of cybercrime. This paper is intended to contribute to this understanding by providing a coherent and accessible understanding of cybercrime, its meaning and associated problems for investigation teams, bringing the knowledge and experience of psychology, social and computing sciences to practitioners and other interested parties. Victims need guidance on who to report cybercrimes to, as do authorities who pass them between organisation or departments with little apparent interest (Button et al., 2020; Cross et al., 2016; HMIC, 2015; HMICFRS, 2019; Holt et al., 2015). Increased availability and clarity of advice regarding cybercrime using a universal lexicon across all relevant bodies (e.g. police, Action Fraud, financial institutions and websites), greater prominence of cybercrime on the Action Fraud website and a more appropriate name such as 'National Fraud and Cybercrime Reporting Centre' are all steps proposed to help mitigate this confusion (Button et al., 2020).

While most police officers perceive cybercrime as serious, equivalent to offline crime, and underestimated by the public, the prevalence of cybercrime is considered lower than that of traditional crime and the perceived frequency of different cybercrimes is inaccurate (Holt et al., 2019). These imprecise views of seriousness and frequency also vary according to officer demographics and experience, suggesting that systematic training and education are required to increase and standardise understanding (Holt et al., 2019). Indeed, government reports assert that knowledge about good practice is not disseminated through local forces efficiently, resulting in inconsistent policing (HMICFRS, 2019).

Improved knowledge of cybercrime, and those involved in it, may improve evidence collection and interviewing, with greater information gleaned increasing likelihood of conviction and prevention. Further research into targeting and victimisation processes, the pathway to committing cybercrime and the associated drift between benign and malicious online activities, as well as current officer interviewing techniques and difficulties, could contribute to the development of an improved training strategy to increase and standardise knowledge, response and investigative empathy.

The value of training has been noted in the literature, including reports from officers themselves who recognise that training is a driving force in perceptions of preparedness to deal with cybercrime investigations and victims (Burruss et al., 2019). However, officers report that such training, and the time provided to take part, is currently insufficient (Forouzan et al., 2018; HMIC, 2015).This is reflected in the perception of victims who are often unsatisfied with their reporting experiences (Button et al., 2020; Cross et al., 2016; HMIC, 2015; Jansen and Leukfeldt, 2018; Leukfeldt et al., 2020).

The needs of cybercrime victims are the same as those of victims of traditional crimes, but, in the former, these needs are often not met (Button et al., 2020; Leukfeldt et al., 2020). Critical to this shortfall is the way in which authorities initially fail to recognise and acknowledge the cybercrime victim – an issue which could be improved with standardised training. Victims describe not being acknowledged as a victim of crime, not being taken seriously, being blamed for their own victimisation and treated with a perceived lack

of dignity and respect (Button et al., 2020; Cross et al., 2016; HMIC, 2015; Jansen and Leukfeldt, 2018; Leukfeldt et al., 2020). Once a crime is recorded, victims report that responding officers appear not to understand the crime, victims are not kept informed about the investigation (or if it is being pursued) and are not offered appropriate support or signposting to external support services (Button et al., 2020; Cross et al., 2016; HMIC, 2015; Jansen and Leukfeldt, 2018; Leukfeldt et al., 2020).

Research shows that immediately following victimisation, interest in cybersecurity is increased, but without the provision of suitable advice and information or signposting to relevant parties, this usually fails to translate into significant behavioural change towards protective routines; demonstrating a missed opportunity to reduce cybercrime (Button et al., 2020). By training officers on the nature and impact of cybercrime, standardising responses, and providing clarity over investigative responsibility, the needs of victims could be met with greater success at the point of report, during and after investigation. This could, in turn, improve reporting rates which remain low due to perceptions that the police are ill-equipped and will not act on victim reports (Button et al., 2020; HMIC, 2015).

Summary and conclusions

Due to perceptions of anonymity and distance from the offline world, internet users experience a false sense of security, and online offenders are psychologically, socially and physically further removed from their offences and victims, encounter fewer and/or less severe consequences for their behaviours and are likely to repeat these offences, emboldened by their experience. Victims of cybercrime under-report their victimisation in comparison to traditional crimes, proposed to stem from a perceived lack of understanding and preparedness in the police, and both victims and police express confusion over which organisation to report to. Training to increase knowledge and provide standardised responses to reports of cybercrime, as well as increased public engagement and signposting, may help improve reporting rates and experiences. Increased knowledge about cybercrimes and those involved may also improve investigative preparedness and increased ability to empathise with victims and suspects to obtain better results at interview, generate more accurate leads and identify appropriate evidence.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This work is part of the CRITiCal project (Combatting cRiminals in The Cloud – funded by the Engineering and Physical Sciences Research Council [EP/M020576/1]).

ORCID iDs

Joanna Curtis https://orcid.org/0000-0002-8279-6166
Gavin Oxburgh https://orcid.org/0000-0003-4830-1673

Notes

1. Sextortion refers to extortion or blackmail based on threats to reveal evidence of sexual activity or any sexual proclivities considered embarrassing or unacceptable.
2. CREST is known almost exclusively by its acronym: www.crest-approved.org/.
3. As calculated using number of reported crimes (2,009,125: Table A4) as percentage of total estimated victims (3,690,000: Table A1) available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.
4. As calculated using number of reported crimes (740,845: Table A4) as percentage of total estimated victims (4,840,000: Table A1) available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.

References

Action Fraud (2020a) *Frequently Asked Questions*. Action Fraud. Retrieved from: https://www.actionfraud.police.uk/faq (Accessed 27 May 2020).

Action Fraud (2020b) *Medical Scams*. Action Fraud. Retrieved from: https://www.actionfraud.police.uk/a-z-of-fraud/medical-scams

Bada M and Nurse JR (2020) The social and psychological impact of cyberattacks. In: *Emerging Cyber Threats and Cognitive Vulnerabilities*. Cambridge: Academic Press, 73–92.

Barnes SB (2006) A privacy paradox: social networking in the United States. *First Monday* 11(9).

Bocij P and McFarlane L (2003) Cyberstalking: the technology of hate. *The Police Journal* 76: 204–221.

Bonta J and Andrews D (2017) *The Psychology of Criminal Conduct*. 6th edition. Oxfordshire: Routledge.

Bossler AM, Holt TJ, Cross C, et al. (2019) Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. *Security Journal* 33: 1–18. DOI: 10.1057/s41284-019-00187-5

Brown CSD (2015) Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9(1): 55–119.

Burruss G, Howell CJ, Bossler A, et al. (2019) Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis", Policing. *An International Journal* 43(1): 105–119. DOI: 10.1108/PIJPSM-08-2019-0142

Button M, Sugiura L, Blackbourn D, et al (2020) *Victims of Computer Misuse: Main Findings*. Portsmouth: University of Portsmouth.

Caneppele S and Aebi MF (2019) Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice* 13(1): 66–79.

Chiesa R, Ducci S and Ciappi S (2008) *Profiling Hackers*. Houston: Auerbach Publications.

College of Policing (2020) *Investigation Process*. Retrieved from: https://www.app.college.police.uk/app-content/investigations/investigation-process (Accessed 27 May 2020).

CREST (2015) *Identify, Intervene, Inspire Helping Young People to Pursue Careers in Cyber Security, Not Cyber Crime*. Retrieved from: https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf

Criminal Law Reform Now Network (2020) *Reforming the Computer Misuse Act 1990. Criminal Law Reform Now Network Report*. CLRNN. http://clrnn.co.uk/publications-reports

Cross C, Richards K and Smith RG (2016) The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice* 518: 1–14.

Curtis J, Oxburgh G and Briggs P (2022) Heroes and hooligans: the heterogeneity of Video Game Modders. *Games and Culture* 17(2): 219–243. http://doi.org/10.1177/15554120211026255

Denning DE (2011) Cyber-conflict as an emergent social problem. In: Holt TJ and Schell B (eds) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, PA: IGI-Global. 170–186.

Dodge C and Burruss G (2019) Policing cybercrime. In: Leukfeldt R and Holt TJ (eds) *The Human Factor of Cybercrime*. Oxfordshire: Routledge.

Downs JS, Holbrook MB and Cranor LF (2006, July 12-14) Decision strategies and susceptibility to phishing. In: Proceedings of the second symposium on usable privacy and security. Pittsburgh, PA, USA: ACM, pp. 79–90.

Dubord P (2008) Investigating cybercrime. In: Barbara JJ (ed) *Handbook of Digital and Multimedia Forensic Evidence*. Totowa, NJ: Humana Press Inc, 77–89.

Farrell G, Laycock G and Tilley N (2015) Debuts and legacies: the crime drop and the role of adolescence-limited and persistent offending. *Crime Science* 4(1): 1–10.

Forouzan H, Jahankhani H and McCarthy J (2018) An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the metropolitan police service. In: Jahankhani H (ed) *Cyber Criminology*. Advanced Sciences and Technologies for Security Applications. Cham: Springer.

Furnell S (2010) Hackers, viruses and malicious software. In: Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. Oxfordshire: Taylor & Francis, pp. 173–193.

Furnell S and Dowling S (2019) Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice* 5: 13–26.

Gaia J, Ramamurthy B, Sanders G, et al. (2020, January 7-10) Psychological profiling of hacking potential. In: Proceedings of the 53rd Hawaii International Conference on System Sciences. Wailea, HI, pp. 2230–2239. DOI: 10.24251/HICSS.2020.273

Gerber N, Gerber P and Volkamer M (2018) Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77: 226–261.

Goldsmith A and Brewer R (2015) Digital drift and the criminal interaction order. *Theoretical Criminology* 19(1): 112–130.

Goldsmith A and Wall DS (2019) The seductions of cybercrime: adolescence and the thrills of digital transgression. *European Journal of Criminology* 19: 98–117. DOI: 10.1177/1477370819887305

Goode S and Cruise S (2006) What motivates software crackers? *Journal of Business Ethics* 65(2): 173–201.

Goodman MD and Brenner SW (2002) The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology* 10(2): 139–223.

Hadlington L, Lumsden K, Black A, et al. (2018) A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice* 15: 34–43.

Harbinson E and Selzer N (2019) The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice* 42(5): 582–598.

Her Majesty's Inspectorate of Constabulary (HMIC) (2015) *Real Lives, Real Crimes: A Study of Digital Crime and Policing*. Justice Inspectorates. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) (2019) *Cyber: Keep the Light on. An Inspection of the Police Response to Cyber-dependent Crime*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf

Hinduja S and Patchin JW (2008) Cyberbullying: an exploratory analysis of factors related to offending and victimization. *Deviant Behavior* 29(2): 129–156.

HM Government (2016) *National Cyber Security Strategy 2016 to 2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Holmberg U and Christianson SÅ (2002) Murderers' and sexual offenders' experiences of police interviews and their inclination to admit or deny crimes. *Behavioral Sciences & the Law* 20(1-2): 31–45.

Holt TJ (2007) Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior* 28(2): 171–198.

Holt TJ (2009) The attack dynamics of political and religiously motivated hackers. In: Saadawi T and Jordan L (eds) *Cyber Infrastructure Protection*. New York, NY: Strategic Studies Institute, 161–183.

Holt TJ and Bossler AM (2013) Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice* 29(4): 420–436.

Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20–40. DOI: 10.1080/01639625.2013.822209

Holt TJ and Bossler AM (2015) *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Oxfordshire: Routledge.

Holt TJ, Brewer R and Goldsmith A (2019) Digital drift and the "sense of injustice": counterproductive policing of youth cybercrime. *Deviant Behavior* 40(9): 1144–1156.

Holt TJ, Burruss G and Bossler A (2015) *Policing Cybercrime and Cyberterror*. Raleigh, NC: Carolina Academic Press.

Holt TJ, Leukfeldt R and van de Weijer S (2020) An examination of motivation and routine activity theory to account for cyberattacks against dutch web sites. *Criminal Justice and Behavior* 47(4): 487–505. DOI: 10.1177/0093854819900322

Hutchings A (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change* 62(1): 1–20.

Jansen J and Leukfeldt ER (2018) Coping with cybercrime victimization: an exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology* 2(2): 205–228.

Jewkes Y and Leukfeldt ER (2012) Policing cybercrime. In: Leukfeldt ER and Stol WP (eds) *Cyber Safety: An Introduction*. The Hague: Eleven International Publishers, 253–266.

Jordan T and Taylor P (2004) *Hacktivism and Cyber Wars*. London, England: Routledge.

Kerstens J and Jansen J (2016) The victim-perpetrator overlap in financial cybercrime: evidence and reflection on the overlap of youth's online victimisation and perpetration. *Deviant Behaviour* 37(5): 585–600.

Kirwan G and Power A (2013) *Cybercrime: The Psychology of Online Offenders*. Cambridge: Cambridge University Press.

Kshetri N (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Berlin/Heidelberg: Springer Science & Business Media.

Lee JR, Holt TJ, Burruss GW, et al. (2019) Examining english and welsh detectives' views of online crime. *International Criminal Justice Review* 31(1):

Leibolt G (2010) The complex world of corporate cyber forensics investigations. In: Bayuk J (ed) *CyberForensics*. New York: Springer Science & Business Media, 7–27.

Leukfeldt ER, Kleemans ER and Stol WP (2017) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology* 57(3): 704–722.

Leukfeldt ER, Notté RJ and Malsch M (2020) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders* 15(1): 60–77.

Leukfeldt ER and Yar M (2016) Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behavior* 37(3): 263–280.

Lewis JA (2018) *Economic Impact of Cybercrime—No Slowing Down*. Washington, DC: The Center for Strategic and International Studies (CSIS) Report.

Madarie R (2017) Hackers' motivations: testing schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology* 11(1).

Maddox L, Lee D and Barker C (2011) Police empathy and victim PTSD as potential factors in rape case attrition. *Journal of police and criminal psychology* 26(2): 112–117.

Matza D (1964) *Delinquency and Drift*. New York: Wiley.

Mayor of London (2019) *Questions to the Mayor 20/06/2019: Backlog of Mobile Phones and Computers Awaiting Forensic Analysis*. https://www.london.gov.uk/questions/2019/12159

Mell P and Grance T (2009) The NIST definition of cloud computing. *National Institute of Standards and Technology* 53(6): 50.

Moeckel C. (2019, August 26-29). Examining and constructing attacker categorisations: an experimental typology for digital banking. In Proceedings of the 14th International Conference on Availability, Reliability and Security. Canterbury, UK, (pp. 1–6). DOI: 10.1145/3339252.3340341

Motoyama M, McCoy D, Levchenko K, et al. (2011, November 2-4) An analysis of underground forums. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, Berlin, Germany, pp. 71–80. DOI: 10.1145/2068816.2068824

National Crime Agency (NCA) (2020) *National Strategic Assessment of Serious and Organised Crime*. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file

National Crime Agency (NCA) (2017) *Pathways into Cyber Crime*. National Crime Agency. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file

Nodeland B and Morris R (2020) A test of social learning theory and self-control on cyber offending. *Deviant Behavior* 41(1): 41–56.

Nurse JR (2019) Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: Attrill-Smith A, Fullwood C, Keep M, et al. (eds) *The Oxford Handbook of Cyberpsychology*. Oxford: Oxford University Press.

Nurse JRC and Bada M (2019) The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. In: Attrill-Smith A, Fullwood C, Keep M, et al. (eds) *The Oxford Handbook of Cyberpsychology.* Oxford University Press.

Office for National Statistics (2017) *Crime in England and Wales: Additional Tables on Fraud and Cybercrime*. Year ending December 2016. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Office for National Statistics (2018) *Crime in England and Wales: Additional Tables on Fraud and Cybercrime*. Year ending December 2017. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Office for National Statistics (2019a) *Crime in England and Wales: Additional Tables on Fraud and Cybercrime*. Year ending December 2018. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Office for National Statistics (2019b) *Crime in England and Wales: Appendix Tables*. Year ending June 2019. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

Office for National Statistics (2020) *Nature of Crime: Fraud and Computer Misuse - Appendix Tables*. Year ending March 2020. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

Oxburgh G and Ost J (2011) The use and efficacy of empathy in police interviews with suspects of sexual offences. *Journal of Investigative Psychology and Offender Profiling* 8(2): 178–188.

Oxburgh G, Ost J, Morris P, et al. (2014) The impact of question type and empathy on police interviews with suspects of homicide, filicide and child sexual abuse. *Psychiatry, psychology and law* 21(6): 903–917.

Pastrana S, Thomas DR, Hutchings A, et al. (2018, April 23-27) Crimebb: enabling cybercrime research on underground forums at scale. In: Proceedings of the 2018 World Wide Web Conference, Lyon, France, pp. 1845–1854.

Radianti J (2010, July 18-25) A study of a social behavior inside the online black markets. In: 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies. Venice, Italy, IEEE, pp. 189–194.

Reep-van den Bergh C and Junger M (2018) Victims of cybercrime in Europe: a review of victim surveys. *Crime Science* 7(1): 1–15.

Reyns BW (2015) A routine activity perspective on online victimisation: results from the Canadian General Social Survey. *Journal of Financial Crime* 22(4): 396–411.

Reyns BW, Randa R and Henson B (2016) Preventing crime online: identifying determinants of online preventive behaviours using structural equation modelling and canonical correlation analysis. *Crime Prevention and Community Safety* 18(1): 38–59.

Richie M and Freiburger TL (2014) Creating identity on social network sites. In: Marcum CD and Higgins GE (eds) *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press, 9–26.

Samtani s, Chinn R and Chen H (2015, May 27-29) Exploring hacker assets in underground forums.In: 2015 IEEE international conference on intelligence and security informatics (ISI), Baltimore, MD, USA, pp. 31–36. IEEE.

Schaefer BP (2014) Social networks and crime: applying criminological theories. In: Marcum CD and Higgins GE (eds) *Social Networking as a Criminal Enterprise*. Boca Raton, FL: CRC Press, 27–48.

Seebruck R (2015) A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation* 14: 36–45. DOI: 10.1016/j.diin.2015.07.002

Slonje R and Smith PK (2008) Cyberbullying: another main type of bullying. *Scandinavian Journal of Psychology* 49(2): 147–154.

Skinner WF and Fream AM (1997) A social learning theory analysis of computer crime among college students. *Journal of research in crime and delinquency* 34(4):495–518.

Sood A and Enbody R (2013) Crimeware-as-a-service - A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6(1): 28–38.

Steinmetz KF (2015) Craft(y)ness: an ethnographic study of hacking. *The British Journal of Criminology* 55(1): 125–145. DOI: 10.1093/bjc/azu061

Steinmetz KF (2016) *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: NYU Press, Vol. 2.

Suler J (2004) The online disinhibition effect. *Cyberpsychology & Behavior* 7(3): 321–326. DOI: 10.1089/1094931041291295

Sykes GM and Matza D (1957) Techniques of neutralization: a theory of delinquency. *American sociological review* 22(6): 664–670.

Turgeman-Goldschmidt O (2005) Hackers' accounts: hacking as a social entertainment. *Social Science Computer Review* 23(1): 8–23.

van de Weijer SG, Leukfeldt R and Bernasco W (2019) Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16(4): 486–508.

Wall D (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press, Vol. 4.

Wall D (2013) Policing identity crimes. *Policing and Society: An International Journal of Research and Policy* 23(4): 437–460.

Wall DS (2017a) Crime, security and information communication technologies: the changing cybersecurity threat landscape and its implications for regulation and policing. In: Brownsword R, Scotford E and Yeung K (eds) *The Oxford Handbook on the Law and Regulation of Technology*. Oxford: Oxford University Press.

Wall DS (2017b) Towards a conceptualisation of cloud (cyber) crime. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Cham: Springer, 529–538.

Weulen Kranenbarg MW, Ruiter S, Van Gelder JL, et al. (2018) Cyber-offending and traditional offending over the life-course: an empirical comparison. *Journal of Developmental and Life-Course Criminology* 4(3): 343–364.

Woo HJ, Kim Y and Dominick J (2004) Hackers: militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology* 6(1): 63–82.

Yar M and Steinmetz KF (2019) *Cybercrime and society* sage.

Zhang L, Young R and Prybutok V (2007) Inhibitors of two illegal behaviors: hacking and shoplifting. *Journal of Organizational and End User Computing* 19(3): 24–42.