THE JOURNAL OF CONCURRENT DISORDERS

CDS PRESS

Open Access Policy Paper

Cybercrimes in the aftermath of COVID-19: Present concerns and future directions

Magdalene Ng, PhD[1*], B. Kennath Widanaralalage, PhD[1], Tom Buchanan, PhD[1], Kovila Coopamootoo, PhD[2]

Citation: Ng, M., Widanaralalage, B.K., Buchanan, T., Coopamootoo, K. (2023). Cybercrimes in the aftermath of COVID-19: Present concerns and future directions. Journal of Concurrent Disorders, 5(2), 35-53.

Founding Editor-in-Chief: Masood Zangeneh, Ph.D.

Editor: Dean Fido, Ph.D.

Received: 10/27/2022
Accepted: 12/22/2022
Published (Online First): 12/23/2022

[1]University of Westminster, UK
[2]Kings College London, UK
ORCiD: https://orcid.org/0000-0002-9914-4586
*Corresponding author: Magdalene Ng, ngm1@westminster.ac.uk

Abstract. Cybercrimes are broadly defined as criminal activities carried out using computers or computer networks. Given the rapid and considerable shifts in Internet use and the impact of the COVID-19 pandemic on cybercrime rates, online behaviours have attracted increased public and policy attention. In this article, we map the landscape of cybercrime in the UK by first reviewing legislation and policy, as well as examine barriers to reporting and address investigative challenges. Given the indisputable rise in cybercrime and its mental health impacts, we propose a four-facet approach for research and practice in this field with an eye to systemic shifts and strategies to combat cybercrime holistically: community alliances and social support, state intervention, and infrastructural sensitivity to user diversity. Lastly, empirical evidence from research guides the design of data-driven technology and provision of advice/interventions to provide a safer digital landscape — hence the importance for more informative research.

Keywords: Cybercrime, Mental Health, Technology, COVID-19, Policy.

Introduction

Cybercrimes are a surging subset of crimes with severe financial, social, and mental health consequences (Ahe, 2022; Bada & Nurse, 2020). Whereas traditional crimes are reportedly decreasing in most Western countries, cybercrimes are expanding (Caneppele & Aebi, 2019). Cybercrimes cross national borders and can have an international dimension, catapulted by the recent push for digital access and services. Cybercriminals may exploit technology by using computer networks to commit crime on a global scale. International examples demonstrate the global reach of cybercriminal hotspots in developing countries (Kshetri, 2019) as far as the UK (Baylon & Antwi-Boasiako, 2016), with damages setting the global economy back by £8.5 trillion per annum by 2025 (Interpol, 2021). Cybercrime is an umbrella term involving cyber-dependent and cyber-enabled crimes, including those offences which can only be committed using online devices or those which represent and escalation of "traditional" crimes through the use of computers (Phillips et al., 2022).

The Tripartite Cybercrime Framework (TCF) offers an interesting classification of cybercrimes across three facets that demonstrate their potentially diverging goals; (i) socio-economic cybercrimes which are computer-mediated with monetary gain acquired or attempted under false representations (examples include online fraud, credit card fraud, online embezzlement and romance scams), (ii) psychosocial cybercrime which are psychologically-driven to cause shock, distress or harm to an individual and where financial benefits are not the main goal (examples include cyberstalking, cyberbullying and online harassment), and (iii) geopolitical cybercrimes which are politically-based with the goal of disrupting and undermining national security/infrastructures (examples include cyber-espionage and malware attacks) (Ibrahim, 2016; Lazarus, 2019).

Prevalence of cybercrimes

Whilst the Office for National Statistics (ONS) does not hold exact information relating to cybercrimes in the UK, some information can be extracted from the Crime Survey for England and Wales (CSEW) and police records regarding computer misuses as well as fraud recorded online. In the year ending March 2021, 1,749,000 computer misuses incidents were recorded. Due to the COVID-19 pandemic, the CSEW was paused, and a telephone-operated version of the survey was implemented (TCSEW). Whilst the ONS advises that the data is not directly comparable with previous version from the CSEW due to the methodological differences, it is noteworthy that in the CSEW for the year ending March 2020, the number of recorded computer misuses incidents was 876,000 (CSEW, 2021). The figures suggest a 99.6% increase in cyber-enabled offences during the period of national restrictions in England and Wales. In relation to fraud, 58% of these offences were cyber-enabled (ONS, 2022). This drastic

increase indicates a growing problem that is pervasive as the Internet is prevalent. Critically, this also highlights a lowered the barrier of accessibility to victims as well as a gap between an emerging phenomenon and empirically-based strategies to combat it.

Further information relating to incidence rates can be gathered from Action Fraud, the UK National Fraud and CyberCrime Reporting Centre. Drawing from this database, Buil-Gil et al. (2021) concluded that most cyber-dependent and cyber-enabled crimes[1] increased between May 2019 (7930) and May 2020 (11,359), particularly for hacking of personal computers, social media, email accounts, and online fraud. The authors also observed that such increases targeted mainly individuals rather than organisations, with cyber-dependant crimes against individuals peaking in April-May 2020, which had the most stringent COVID-19 restrictions nationwide. Buil-Gil and colleagues (2021) report that the shift from physical to online environments create a wealth of opportunities for cyber-dependent and enabled crimes, also giving rise to new COVID-related scams (Bergeron et al., 2020; Monteith et al., 2021; Pasculli, 2020).

This documented shift is particularly concerning, given the long-standing and broad-spectrum of mental health and emotional impacts of cybercrimes across society which are evidently equally and perhaps even more severe than the financial impact (Modic & Anderson, 2015). Cybercrime victims have reported emotional trauma (Bergmann et al., 2018) leading to depression, acute stress, anger, feeling violated, and powerlessness (Bada, 2020), and physical illness (Dong & Simon, 2013), with some reports even suggesting hospitalisations (Dong & Simon, 2013). Monteith and colleagues (2021) report how existing mental health concerns can worsen, where double victimisation and relapses can occur (Whitty & Buchanan, 2016). The underpinning mechanisms following an economic shock is a loss of trust, triggering self-blame (Whitty & Buchanan, 2016) – which in turn impacts health and how victims perceive themselves, corroding their self-esteem (Bailey et al., 2019) especially if resorting to maladaptive coping strategies (Bailey et al., 2019).

These impacts of cybercrimes are, evidently, of public and policy interest. Therefore, the present article will discuss current legislation, reporting and investigative issues, followed by a focus on how to tackle some of these challenges. We conclude by proposing a recommended ecosystem of forces that involves collaborative measures taken by multiple forces ranging from the government to individuals. Whilst our discussion primarily focuses on UK policy and legislations, the proposed strategies are not exclusive and provide valuable insight for other countries.

Legislation in England and Wales

The recent case of 14-year-old Molly Russell's death highlights a gap between law and technological advancements, leading public figures to call for a reform of digital policy issues for children and young people (Andersson, 2022), where the legislations should have equivalent capacity

to react to and confront these threats (Hunton, 2010). A concern relating to the definition and study of cybercrimes is the absence of a comprehensive cybersecurity law in England and Wales. Instead, cybercrimes are legislated across a wide range of legislations, which include an issue relating to the definition and study of cybercrimes is the absence of a comprehensive cybersecurity law in England and Wales. Instead, cybercrimes are legislated across a wide range of legislations, which include (i) the Data Protection Act (DPA) 2018 with the EU General Data Protection Regulation, where the DPA regulates data protections requirements for national security and immigration, (ii) the Investigatory Powers Act 2016 which regulates surveillance and unlawful interception of communications data, (iii) the Computer Misuse Act 1990 which describes a series of offences which constitute cybercrime, and can be prosecuted alongside other legislations on Theft and Fraud, and (iv) the Fraud Act 2006 which regulates offences by false representations, failure of disclosure, and abuse of position.

Table 1: examples of cybercrime, relevant legislation, and maximum penalties

Type of cyber-enabled and dependant crime	**Relevant legislation**	**Maximum penalties**
Hacking	Computer Misuse Act 1990[2]	2 years imprisonment
	Investigatory Powers Act (IPA) 2016[3]	Summary conviction (fine)/conviction on indictment (2 years imprisonment/fine/both)
	Data Protection Act 2018[4]	£17.5m/4% annual global turnover
Denial-of-service attacks (including malware, ransomware, spyware, and viruses)	Computer Misuse Act 1990	10 years imprisonment
Phishing Identity theft/fraud	Fraud Act 2006[5]	10 years imprisonment

The UK Parliament introduced an Online Safety Bill (2021), a draft regulatory framework designed to detail user-to-user services' duty of care in the UK. For example, platforms will be required to remove illegal and "legal but harmful" content. Critically, while the Bill, which has passed first reading, strengthens safeguards against certain cybercrimes, such as hate crimes and harassment, and protects UK citizens, it does not extend to financial cybercrimes (Burton et al., 2022).

The dark figure of cybercrime

The dark figure of cybercrime is well-acknowledged, in that victims of cybercrimes are far less likely to report their victimisation to the police compared to the actual rate that the crime occurs (Curtis & Oxburgh, 2022). Cybercrime reporting tends to be low for various reasons (Button, 2014; Cross, 2016). One critical reason for this lack of engagement with the criminal justice system is a predisposition to distrust authorities and a lack of confidence that law enforcement agents are able to and are prepared to actually solve the cybercrime (DeLiema, 2018). Victims also report feeling ignored, embarrassed, and ashamed (Burton et al., 2022; Curtis & Oxburgh, 2022), and often do not want to appear on the 'sucker list' (a list of those who have previously fallen for a cybercrime) (Cross et al., 2014). Cybercriminals use the use details on this list to target and re-victimise this at-risk group of individuals, sometimes even selling this detail to other offenders.

A clear lack of a central cybercrime reporting unit is another reason for low reporting of cybercrimes (Curtis & Oxburgh, 2022). A case in point, while individuals are directed to seek advice from the National Cyber Security Centre (NCSC) for phishing, they are instructed to report misleading adverts and scams to Advertising Standards Authority. However, for online scams or frauds they are directed to either Action Fraud (in England, Wales and Northern Ireland), the police, or Crimestoppers (Curtis & Oxburgh, 2022) — highlighting a lack of a centralised reporting system which sustains confusion in the reporting process.

Curtis and Oxburgh (2022) demonstrate that police officers themselves express confusion over which organisation cybercrime victims should report to, at times turning cybercrime victims away by erroneously informing them that they are not victims of a criminal offence. This is also in part due to the lack of comprehensive cybercrime laws in the police force about what constitutes a cybercrime (Hadlington et al., 2018). Curtis and Oxburgh (2022) further highlight jurisdictional issues in cybercrimes where uncertainty lies within law enforcement agencies as to whose role it is to investigate, be it the police, Action Fraud, organisations such as the National Fraud Investigation Bureau (NFIB) or the National Crime Agency (NCA), third party companies involved such as financial institutions, service providers or insurers. These present as barriers to reporting and investigative challenges, which we will address in the sections below that may help to renew public confidence and trust in the police.

Future directions

As shown above, cybercrime is layered and divided across different socio-economic, psychosocial, and legislative motivations (Ibrahim, 2016; Lazarus, 2019). Therefore, we propose a four-facet approach in adopting a responsibilisation strategy for population-level change (Horgan et al., 2021). These four facets reflect a co-creation of solution, which includes

shared responsibility of businesses, technology, legal stakeholders, responsible research, alongside individual users. This is illustrated in Figure 1 in the responsibilities that civil society holds (personal guardianship and community support), and those held by organisations, academia, and the government (state interventions, evidence-based research and infrastructural sensitivity to user diversity) (Pasculli, 2020). We argue that risk of vulnerability to cybercrime is minimised where these four facets interact and overlaps, mapping onto the work that is being carried out by the Research Institute for Sociotechnical Cyber Security (RISCS) in shared digital responsibilisation[6]. We expound on each facet accordingly.

Figure 1: Four facets of shared cybercrime responsibilisation and minimisation of vulnerability

Personal guardianship

Given the sudden and rapid shift online described in this paper, the need for higher levels of technical and technological knowledge is increasing (Monteith et al., 2021), whereby users can, proactively, safeguard their online safety and digital identities. Such actions fall under personal guardianship and are aimed at preventing losses such as privacy, data, and finance (Lee et al., 2008; Mohamed & Ahmad, 2012). The concept of guardianship stems from routine activity theory (RAT), first introduced by Cohen and Felson in 1979 (Cohen & Felson, 2010), which has since been

applied to cybercrime (Burton et al., 2022; Chen, 2017; Reyns, 2013). The theory posits that crime is likely to occur when essential elements of crime converge in space and time, one of which is the lack of a capable guardian. As such, in the context of online and digital safety, personal guardianship includes using and updating antivirus, antitracking, antispyware and antimalware software regularly, using strong passwords, changing passwords regularly, using VPN/Proxy, using private browsing, adjusting privacy and security settings on sites, filtering (HTTPS) sites, clearing cookies, the use of pseudonyms and encryption (Lee et al., 2008; Mohamed & Ahmad, 2012).

Critically, protective behaviours are not always equally effective similarly across all cybercrime type and protection for specific cybercrimes needs consideration. For example, having protective software (such as an updated antivirus/spybot/ad-aware software, and having software/hardware firewalls) will not protect against cyber-abuse or romance scams (Redmiles et al., 2017). Despite knowledge of online self-protective behaviours, those most at-risk of cybervictimisation underuse or do not effectively use online protective strategies (Drew & Farrell, 2018) or utilise simple non-technological methods that do not effectively shield against certain types of cybercrime (Coopamootoo, 2020). Research has consistently found that the average online user often does not possess sufficient cyber knowledge (Coopamootoo, 2020), highlighting the notion that humans are the weakest link in cybersecurity (Goh, 2021) for a variety of reasons including being unaware of risks, little experience with social and technical protection methods, no awareness of protection tools and no perceived need to act (Coopamootoo, 2020). Most individuals do not use best practices to protect their passwords or defend themselves against online attacks (Cain et al., 2018), or even perceive such attacks as a threat to themselves and, if they do, they believe that there is very little that they can do to prevent such an attack (Bada & Nurse, 2019). Given this knowledge, the burden of protection cannot fall on users alone, especially when considering vulnerable individuals.

Facet 1: Community alliances and social support

Personal guardianship and responsibilisation of the user is necessary but not sufficient to minimise online harm. Having someone else available nearby can sometimes be effective in preventing cybercrimes from taking place. Merely being present can play a part in deterring a cybercrime attack by acting as a capable cyberguardian (Nicholson et al., 2020), a type of social support. The role of cyberguardians as a steward can include promoting conversations about enhancing cyber-protective behaviours, sharing personal stories and sources of threats online from personal experience through opportunistic information sharing (Nicholson et al., 2020). They spread and advocate best cybersecurity information within communities by a peer-to-peer sharing method. RAT also applies here, for example, an individual is more exposed to cybercriminals if they have a

recently bereaved partner who used to manage finances and they are now assuming unfamiliar online activities while simultaneously having less access to support and advice (Burton et al., 2022).

Besides methods of personal guardianship methods and an assigned or active cyberguardian, an individual can seek help through other avenues of social guardianship (such as through family, friends, acquaintances, co-workers, and peers) for cybersecurity advise in everyday life (Murthy et al., 2021). This channel is mainly through one's social connections and sometimes within one's household itself — prevalent source of cybersecurity advice. Because it is easily available due to its social/informal nature (such as through "gossips" about what happened to their neighbour in an incident involving threats of cybercrime), it is perceived as helpful. Social guardianship can also take a formal route, including dedicated IT departments in the workplace, organisations, public bodies publicising and enforcing training, and education to employees or implementing strict regulations as a form of cyberguardianship (Rader & Wash, 2015). Voluntary society groups and community-based entities such as charities may provide targeted support and advice to vulnerable groups by helping them understand how to protect themselves and become safer digital citizens.

Facet 2: State intervention

While we strongly advocate for individual (and private organisations) action, this alone cannot combat cybercrime in their entirety. The state can play a major role in keeping its citizens safe online. An example of state intervention involves dissemination of online best practices through government webpages. UK's National Cyber Security Centre (NCSC)'s website provides a list of best practices online such as using more than one type of Firewall to secure internet connection, choosing the most secure settings for devices and software, controlling who has access to personal data and services, installing anti-malware protections, as well as regularly updating software. Similarly, also available publicly is the Cyber Security Body of Knowledge (CyBOK), which is a handbook of best practices in security and privacy behaviours. This catalogues protective methods from victims' perspectives (Rashid et al., 2018).

That said, much has yet to be done in this area. An in-depth examination reveals that UK police officers report great difficulties in investigating cybercrimes (Hadlington et al., 2018). The threat from cyber-dependent crime is often not fully understood and is hardly seen as a priority (HMICFRS, 2019). Police officers often struggle to empathise with victims as well as suspects of cybercrimes because cybercrimes fit the idea of a faceless crime due to the anonymity and invisibility of offenders (Black et al., 2019; Lusthaus & Varese, 2017), highlighting investigative challenges and frustrations related to a lack of knowledge and power to deal with cybercrimes (Curtis & Oxburgh, 202; Hadlington et al., 2018). This is a critical finding because it demonstrates where support can be given to law

enforcement agents in this area to improve investigative preparedness and to be able to better provide state-level guardianship to UK citizens.

This calls for specialist training delivered by cybercrime experts (Hadlington et al., 2018) because interviewing cybercrime victims differs from other types of crime interviewing[7]. While many aspects of cybercrimes happen offline and the general methods of these investigations are similar to traditional investigations (Carrier & Spafford, 2003), the digital investigation procedure involves computer systems and therefore requiring specialised knowledge of technology, systems, an ability to extract evidence from potential sources, data acquisition and recovery, determining relevance of digital evidence, knowledge of handling of evidence, and analysis of this data (Carrier & Spafford, 2003; Hunton, 2010). This also involves investigators working together with and communicating with digital forensic investigators (DFIs) who are tasked with collecting the right evidence from the victim or cybercriminal(s). Police will also benefit from training in what digital evidence to collect, and being trained in techniques to elicit technical information surrounding the crime and impacts on cybercrime victim's cognitive function and memory retrieval from use of digital devices, in parallel with proper handling and documentation of electronic evidence.

Together with a unified (understanding of the) reporting process, offering structured learning opportunities on state-of-the-art cybercrime knowledge (such as learning about technological developments in malwares and ransomwares) and training on domain knowledge of legislation as well as policies that cybercrimes cover, would further aid police officers in conducting cybercrime and digital investigations. Understandably, cybercrimes lacked a consensus in definition until recently, with individual, institutional and organisational differences in operationalisation of the term (Phillips et al., 2022). Therefore, training by experts in the field would serve the police better with regard to the parameters of cybercrimes and the layers of cyberspace. Changes in organisational structures are also necessary to provide the necessary capacity, capabilities, and partnerships to increase police confidence, possibly involving the formation of specialised cybercrime units (Willits & Nowacki, 2016). Being aware of this issue allows a weighted allocation of police resources to this area (Bidgoli & Grossklags, 2016).

Government-commissioned reports reveal inadequate aftercare to support cybercrime victims in UK (Button et al., 2020). We advocate for the centrality of victim-focused care, focussing on advice for and recovery of mental health traumas cybercrime victims face (Cross et al., 2016). To change the perception that victims of cybercrimes currently have of police officers being ill-equipped to handle cybercrime offenses (Curtis & Oxburgh, 2022) and ensure they receive a good quality response, police officers need to provide standardised responses to reports of cybercrime. This standardised response includes following an interviewing protocol, guide or training material derived from research, and also includes not

having an 'ideal' victim mindset – acknowledging and not dismissing victims, as well as understanding the threat and risks victims face (Black et al., 2019; Curtis & Oxburgh, 2022). We advocate for empathy training (Gabbert et al., 2021) to increase police officers' ability to empathise with victims and suspects to generate more accurate information and to identify evidence. During interviewing, care should be taken not to stigmatise victims by changing the language to cybercrime "survivor" in order to normalise victimisation and to cease self-blame (Peng, personal communication, July 18, 2022).

Responding to victims effectively also means signposting to support agencies and referral services, providing the right advice to access cybersecurity toolkits through a centralised guidance and information site, giving updates on investigation leads (Curtis & Oxburgh, 2022), and recommending a government-approved list of trusted sources on cybersecurity information (Monteith et al., 2021). This helps curb confusion, may prevent re-victimisation, while taking into consideration their mental, physical and emotional trauma – all of which aligns with the trauma-informed and victim-centred approach (Chenier et al., 2021). By having a point of contact for information about their case, this can increase their confidence in police and/or services capability and duty of care in parallel. Changes to a user-friendly reporting system, protect-by-design characteristic (Burton et al., 2022), can further lend support for cybercrime victims. Having a visible reporting section on sites increases transparency and can encourage increases in reporting.

Facet 3: Infrastructural sensitivity to user diversity

Besides community alliances, individual guardianship, and the role of the state, there is a need to recognise the broad structural systems that enable cybercrime, which includes organisations' responsibility in handling customers' data and the design of technology being safe as a service before being introduced to a user base (upkeeping industry standards including keeping their security networks safe by working with penetration testers and having defence toolkits in place for attacks, as examples). To this end, technology can reinforce the fight against cybercriminals where existing and future designs of online interfaces can target mechanisms where individual vulnerabilities usually take place to protect users, while built-in countermeasures to cybercrimes within digital devices to be resilient to attacks. Protect-by-design infrastructures with security and privacy benefits in technological products and protective technologies offered by technological companies (NCS, 2022), which can eventually include security and privacy-by-design in cyberspace, akin to the notion of designing-out-crime offline (Me & Spagnoletti, 2015; Whitord, 2018). This has to also involve policymakers and those who can implement these interventions (Pease et al., 2018).

Giving the right solution that is information-relevant and resonant to the right user group is key, due to the diversity of cybercrimes. It is

therefore vital to disaggregate cybercrime types due to their differential impacts on different population groups, and for technological designs and interventions to be built to suit diverse user characteristics. For example, existing technology is often not suited or built for vulnerable users (this would include design interfaces of reporting cybercrimes), such as those who are on the autistic spectrum (Ledingham & Mills, 2015), repeat cybercrime victims (Correia, 2020), and those with executive cognitive and mental illnesses who are at high risk of victimisation online and where guardianship is even more vital (Monteith et al., 2021). Similar cohorts susceptible online due to slower processing and cognitive decline are older adults, often with aggravating comorbid health vulnerabilities (Burton et al., 2022), memory impairments (Ebner et al., 2020) and social isolation (Costa et al., 2020). In parallel, children accessing the Internet are in need of better protection from cases such as sexual exploitation and access to pornography (Online Safety Bill, 2021).

A gendered analysis of cybercrime is also important (Bada et al., 2021), especially because the online space can house hidden gendered power dimensions (Lindén, 2022). Of recent, there has been a push for the application of feminist theories to define, theorise and explore cybercrimes, seeing as cybercrime and cybersecurity have been male-dominated fields (Phillips et al., 2022). Certain cybercrimes such as online harassment (increasingly part of the online dimension of domestic and interpersonal violence) (Lopez-Neira et al., 2019) and cyberstalking (e.g., obscene emails/text messages, ordering unwanted goods or services at victim's expense, taking photos without consent, posting photos or comments online), pose significant problems especially for women (Chahal et al., 2019) with major mental health impacts such as depression, anxiety and sleep disorders (Navarro et al., 2015). Men similarly experience harms online, including image-based sexual violence (Walker et al., 2019). Given the unique pressures experienced by men to disclose any experience of victimisation or seeking support (Addis & Mahalik, 2003; Widanaralalage et al., 2022), the differential and unique impacts of gender cannot be understated, as these are visible in many ways (Bada et al., 2021; Coopamootoo, 2022; Redmiles et al., 2017). One current and important UK government initiative to address Violence Against Women And Girls[8] in digital technology is the Digital, Data and Technology Directorate of the NCA with the aim to address sexism and misogyny in cyberspace.

Infrastructural designs and interventions should also take into account social practices and cultural dynamics. There exists very little cross-cultural research on protective user practices and contextual variances in adoption of protective behaviours and/or contributors to cybervictimisation. This includes how security and privacy is experienced and produced in families and cyberguardianship structures in these communities. There is evidence that highlights that considerable differences exist between end users from different countries (Kigerl, 2016) in levels of cybercrime threat perception, in uptake and levels of compliance in online

cybersecurity behaviours. Levels of digital skills may also vary by country (James, 2021). As another example, the role of culture and its dimensions can be significant influences on how victims behave before, during and after being victimised. This can manifest in differential motivations as to why they report (or otherwise) based on different underlying cultural dynamics. Clearly, these attest the need for support and careful design of cybersecurity technologies that all users from all genders, age groups, sexualities, ethnicities, cultures, disabilities and social classes can confidently engage with. Inclusivity (in terms of gender justice, age, sexuality, ethnicity, culture, disabilities, and social class) and a redress for existing inequalities in the digital sphere is clearly warranted and desirable in the development of strategies to tackle cybercrimes, especially if we consider the implications of the discourses that sustain inequality in cybersecurity (Lindén, 2022).

Facet 4: Evidence-based guidance and data-driven technology

Evidently, the most sophisticated technology, knowledge and tools will not always be sufficient to protect against and even predict cybercrime. Furthermore, it is empirical evidence from research that guides the design of technology to keep individuals safe online. For example, understanding the antecedents of online repeat victimisation through a longitudinal exploration may aid its reduction and prevention through predictive work. Furthermore, data-driven digital technologies can be an influential agent of equality, making headway in breaking the inequality divide. For this reason, calibrating state strategies with academia so that research-driven policies and training can be instigated is essential to effectively manage the continuous rise of cybercrime with the goal of prevention, investigation, and prosecution of these crimes. As such, interdisciplinarity within cybercrime-strategies are a critical starting point.

As the cybercriminal ecosystem and cyberspace are multi-layered and are accessed via different means, we stress the need to bridge (i) cybersecurity, a subset of computer science in understanding data, networks, systems, software, and communication devices, (ii) cyber-criminology (Ngo & Jaishankar 2017), and (iii) cyberpsychology (Monteith et al., 2021; Whitty, 2016) as a step towards driving important changes. While these three fields separately contribute to scientific discoveries in their own right, Dupont and Whelan (2021) aptly point out that these facets are very much detached as of current and in much need of interaction and strategic partnerships. While forensic cyberpsychology is an emerging field that combines the study of cyberpsychology and cybercriminology (Pradeep, 2020), current research by behavioural scientists, social scientists and computer scientists remains a patchwork of efforts. They are largely still disparate and needs more entwined working practices to avoid duplicate efforts and confusion in the field. This will also allow unanimous definitions, greater transparency with combined methodologies for effective collaborations – in being one step ahead of cybercriminals to outpace the

scale and speed of cybercrime growth, especially when new forms of scams are rapidly emerging (e.g., crypto scams) as we head into the era of the metaverse (Mackenzie, 2022) where new types of online crimes can occur.

Conclusion

In this article, we detail the rapid changes in the landscape of cybercrime and the need for practitioners, stakeholders, academics and the public to shift accordingly. Technological advances require an ability to navigate opportunities and challenges in the online space to be more secure and resilient by taking collective, whole-of-society, coordinated actions. The evidence and recommendations presented above emphasise how collective ownership of responsibility at different levels (individual, organisational, and governmental) could help counter cybercrimes more effectively. While government works towards decreasing the cybersecurity burden on citizens, personal and social guardianship play a role in taking reasonable steps to protect not only our devices, our data, software, networks and systems, but also our communities. Indeed, our model for guardianship highlights the importance of openly discussing cybersecurity with family, friends and colleagues, whilst simultaneously recognising the critical need for generating specialised support, care, and advice for cybercrime victims as well as to police officers interviewing cybercrimes.

In our overview of the landscape of cybercrimes in the aftermath of the COVID-19 pandemic, the evidence clearly points towards the necessary and welcomed emergence of forensic cyberpsychology. Research in this area is desperately needed, to bring different components and school of thoughts to ensure that social sciences are not outpaced by the dizzying growth of online technology, practices, and cultures. Indeed, providing evidence-based, multi-disciplinary recommendations to inform regulations to tackle and manage online harms could promote and improve online safety and digital health. Crucially, research (and researchers) in forensic cyberpsychology must strive towards the recognition of different end user-characteristics, by taking an intersectional and inclusive approach that extends beyond WEIRD populations and consider cross-cultural variations that may exist. Clearly, until we recognise the individual, organisational, national, and international impact of cybercrimes, cyberspace will remain another platform that continues to host inequalities.

Notes

[1]Buil-Gil et al. (2021) examined the following cyber-dependent crimes: computer viruses, malware, spyware; denial of service attack; hacking (server, personal, social media and email); hacking combined with extortion; online fraud (shopping and auctions).

[2] https://www.legislation.gov.uk/ukpga/1990/18/contents

[3] https://www.legislation.gov.uk/ukpga/2016/25/contents

[4] https://www.legislation.gov.uk/ukpga/2018/12/contents

[5] https://www.legislation.gov.uk/ukpga/2006/35/contents

[6] https://www.riscs.org.uk/digital-responsibility/

[7] https://www.riscs.org.uk/project/investigative-interviewing-of-cybercrime-victims-to-gain-best-evidence/

[8] https://www.gov.uk/government/publications/responses-to-super-complaint-report-a-duty-to-protect/national-police-chiefs-council-npcc-response-to-recommendations-accessible

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Availability of data and material

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Author's contributions

MN wrote the manuscript, BKW provided data for Table 1 and Prevalence of Cybercrimes. Both MN and BKW conceptualised Figure 1. TB and KC contributed to the Introduction, Figure 1 and the four facets. All authors reviewed the final manuscript.

Conflict of Interest

The authors declare no conflict of interest.

Informed Consent

Informed consent was required for this manuscript.

Ethics Approval

Ethics approval was not required for this manuscript.

References

Addis, M. E., & Mahalik, J. R. (2003). Men, masculinity, and the contexts of help seeking. *American psychologist*, *58*(1), 5.

Ahe, L. (2022). *Mental Wellbeing and Cybercrime (The Psychological Impact of Cybercrime on the Victim)* (Bachelor's thesis, University of Twente).

Andersson, J. (2022, October 1). T Prince William makes online safety plea after Molly Russell verdict. *BBC NEWS.* https://www.bbc.co.uk/news/uk-63097739.

Bada, M., Chua, Y. T., Collier, B., & Pete, I. (2021). Exploring masculinities and perceptions of gender in online cybercrime subcultures. In *Cybercrime in Context* (pp. 237-257). Springer, Cham.

Bada, M & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic Press.

Bailey, J., Kingston, P., Taylor, L., & Eost-Telling, L. (2019). The health impact of scams. *Innovation in Aging*, *3*(Suppl 1), S757.

Baylon, C., & Antwi-Boasiako, A. (2016). Increasing internet connectivity while combatting cybercrime: Ghana as a case study.

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy*, *83*, 102870.

Bidgoli, M., & Grossklags, J. (2016, June). End user cybercrime reporting: what we know and what we can do to improve it. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-6). IEEE.

Black, A., Lumsden, K., & Hadlington, L. (2019). 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim When Responding to Reports of Interpersonal Cybercrime. In *Online Othering* (pp. 355-378). Palgrave Macmillan, Cham.

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2021). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, 111678.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36-45.

Caneppele, S., & Aebi, M. F. (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.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, *2*(2), 1-20.

Chahal, R., Kumar, L., Jindal, S., & Rawat, P. (2019). Cyber stalking: Technological form of sexual harassment. *Int. J. Emerg. Technol*, *10*, 367-373.

Chenier, K., Milne, R., Smith, K., & Snook, B. (2021). Interviewing Adult Complainants in Sexual Assault Cases. *Criminal Investigations of Sexual Offenses*, 67-84.

Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203-232). Routledge.

Coopamootoo, K. P. (2020, October). Usage patterns of privacy-enhancing technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1371-1390).

Costa, M., Pavlo, A., Reis, G., Ponte, K., & Davidson, L. (2020). COVID-19 concerns among persons with mental illness. *Psychiatric Services*, *71*(11), 1188-1190.

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and issues in crime and criminal justice*, (474), 1-6.

Cross, C., Richards, K., & Smith, R. (2016). Improving responses to online fraud victims: An examination of reporting and support (Report to the Criminology Research Advisory Council Grant: CRG 29/13-14).

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, 0032258X221107584.

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activit theory. *The Gerontologist*, *58*(4), 706-718.

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537-549.

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of criminology*, *54*(1), 76-92.
Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of criminology*, *54*(1), 76-92.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D.L., Turner, G.R., Spreng, R.N., & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75*(3), 522-533.

Gabbert, F., Hope, L., Luther, K., Wright, G., Ng, M., & Oxburgh, G. (2021). Exploring the use of rapport in professional information-gathering contexts by systematically mapping the evidence base. *Applied Cognitive Psychology*, *35*(2), 329-341.

Goh, P. (2021). Humans as the weakest link in maintaining cybersecurity: building cyber resilience in humans. In *Introduction to Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators* (pp. 287-305).

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2021). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 34-43.

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-aninspection-of-the-police-response-to-cyber-dependent-crime.pdf.

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*.

Hunton, P. (2010). Cybercrime and security: a new model of law enforcement investigation. *Policing: a journal of policy and practice*, *4*(4), 385-395.

Interpol. (2021, May 12). *New INTERPOL desk targets cybercriminals and Internet fraud in Africa.* INTERPOL. https://www.interpol.int/en/News-and Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa.

James, J. (2021). Confronting the scarcity of digital skills among the poor in developing countries. *Development Policy Review*, *39*(2), 324-339.

Kemp, S. (2020). Fraud against individuals in the Internet era: trends, victimisation, impact and reporting.

Kigerl, A. (2016). Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. *International Journal of Cyber Criminology*, *10*(2).

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81.

Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism*.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454.

Lindén, E. (2022). Gender in Cyber policy, is it really necessary?: A critical analysis of gender in EU's cybersecurity policy.

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G. and Tanczer, L. (2019), "*Internet of things':How abuse is getting smarter*", *Safe – The Domestic Abuse Quarterly*, 63, 22-26.

Lusthaus, J., & Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*, *15*(1), 4-14.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*.

Me, G., & Spagnoletti, P. (2005, November). Situational Crime Prevention and Cyber-crime investigation: the Online Pedo-pornography case study. In *EUROCON 2005-The International Conference on" Computer as a Tool"* (Vol. 2, pp. 1064-1067). IEEE.

Modic, D., & Anderson, R. (2015). It's all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security & Privacy*, *13*(5), 99-103.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, 23(4), 1-9.

Murthy, S., Bhat, K. S., Das, S., & Kumar, N. (2021). Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1-24.

National Cyber Security Centre (NCSC). (n.d.) *Advice and guidance.* NCSC. https://www.ncsc.gov.uk/cyberessentials/overview.

Navarro, R., Yubero, S., & Larrañaga, E. (Eds.). (2015). *Cyberbullying across the globe: Gender, family, and mental health*. Springer.

Ngo, F. T., & Jaishankar, K. (2017). Commemorating a decade in existence of the International journal of cyber criminology: a research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology*, *11*(1),

Office for National Statistics (ONS). (2022, March 15). Cybercrime in the UK 2018-2021. ONS. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-whitepaper.

Okereafor, K., & Adebola, O. (2020). Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Int J IT Eng*, *8*(2).

Pasculli, L. (2020). Coronavirus and Fraud in the UK: From the Responsibilisation of the Civil Society to the Deresponsibilisation of the State. *Lorenzo Pasculli' Coronavirus and fraud in the UK: from the responsibilisation of the civil society to the deresponsibilisation of the state'[2020]*, *25*(2), 3-23.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379-398.

Pradeep, K. P. (2020. Forensic Cyberpsychology in Pandemic Period. *Journal of Forensic Sciences & Criminal Investigation, 14*(3): 555887.

Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, *1*(1), 121-144.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, *16*(3), 96-102.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2017, May). Where is the digital divide? a survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 931-936).

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

Trengove, M., Kazim, E., Almeida, D., Hilliard, A., Zannone, S., & Lomas, E. (2022). A critical review of the Online Safety Bill. *Patterns*, 100544.

Walker, K., Sleath, E., Hatcher, R. M., Hine, B., & Crookes, R. L. (2021). Nonconsensual Sharing of Private Sexually Explicit Media Among University Students. Journal of Interpersonal Violence, 36(17–18), NP9078–NP9108. https://doi.org/10.1177/0886260519853414.

Widanaralalage, B. K., Hine, B. A., Murphy, A. D., & Murji, K. (2022). "I didn't feel I was a victim": a phenomenological analysis of the experiences of male-on-male survivors of rape and sexual abuse. *Victims & Offenders*, 1-26. https://doi.org/10.1080/15564886.2022.2069898.

Whitford, T. (2018). Cyber defense for IMGs and NGOs using crime prevention through environmental design. In *Cyber Weaponry* (pp. 47-58). Springer, Cham.

Whitty, M. T. (2017). *Cyberpsychology: The study of individuals, society and digital technologies*. John Wiley & Sons.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal justice studies*, *29*(2), 105-124.