Volume 1, Issue 1 (2023)

ISSN: 2959-3018 (print) / 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

The Commonwealth Cybercrime Journal

The Commonwealth

Foreign, Commonwealth
& Development Office

Editors-in-Chief

Dr Nkechi Amobi and Dr Tawanda Hondora
The Commonwealth Secretariat
Marlborough House
Pall Mall
St. James's
London SW1Y 5HX
United Kingdom

n.amobi@commonwealth.int /
cybercrime@commonwealth.int

Editorial board members

Advisory board

About the journal

The Commonwealth Cybercrime Journal (CCJ) is published by the Commonwealth Secretariat as part of the Commonwealth Cybercrime Programme, funded by the UK Foreign, Commonwealth and Development Office to fulfil the objectives of the 2018 Commonwealth Cyber Declaration.

This annual journal provides a platform for policy-influencing articles and commentary by academics, policymakers, practitioners and experts exploring significant cybercrime and cybersecurity issues. Its goal is to promote understanding of both the magnitude of contemporary challenges posed by cybercrime and the actions required to effectively address them.

The journal's areas of focus include but are not limited to: state actors and cyber warfare; ransomware and phishing; proceeds of crime; terrorism, privacy and security of data; intellectual property; infringement and counterfeit; online harassment and cyberstalking; election cybersecurity; virtual courts and electronic evidence; cybersecurity and the economy; digital currencies; and child online safety. Articles published in the journal specifically focus on the Commonwealth region, and/or include case studies in which victims and/or perpetuators of cybercrime are from a Commonwealth country. Article authors are typically drawn from Commonwealth countries.

For full aims and scope, and guidelines for submission, see thecommonwealth.org/cybercrime-journal

The Commonwealth

Contents

D19156

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Editorial

Nkechi Amobi and Tawanda Hondora

Digital technology's rapid evolution is dramatically changing all aspects of human life. The benefits to our education, social, economic, industrial and political systems are immeasurable. Over the past couple of years, the COVID-19 pandemic has been partly responsible for the rapid adoption of digital technologies: the International Telecommunication Union (ITU) has indicated that the number of internet users grew from 4.1 billion in 2019 to 4.9 billion in 2021.[1]

Unsurprisingly, however, this upsurge has been accompanied by an exponential rise in cybersecurity attacks and cybercrime. It is estimated that cybercrime will cost the global economy US$10.5 trillion by 2025,[2] following reports of a 13 per cent increase in ransomware attacks worldwide between 2021 and 2022 – an increase greater than that during the five preceding years.[3] This is most likely an underestimate, as many countries do not have adequate cybersecurity and cybercrime reporting frameworks.

All countries are scrambling to play catchup with cybercriminals and ensure that the internet stays free, open, and inclusive – key ideals adopted by Commonwealth Heads of Government in their 2018 Commonwealth Cybercrime Declaration.

One of the critical impediments to realising these ideals, and to ensuring the safe, secure, effective and efficient use of both new digital technologies and cyberspace more generally, is the paucity of policy-influencing literature. The *Commonwealth Cybercrime Journal* (*CCJ*), published by the Commonwealth Secretariat and fully peer-reviewed, intends to address this.

The *CCJ* features policy-influencing articles, case studies and cutting-edge commentary from leading practitioners, policymakers, experts and academics with the aim of assisting Commonwealth countries – particularly Small Island Developing States – to strengthen their anti-cybercrime legislative, policy, institutional and multilateral frameworks. This will assist countries to uphold the rule of law both online and in the physical world – as the lines between the two become increasingly blurred. In this regard, the *CCJ* serves as a toolkit for policymakers, industry experts, academics and practitioners involved in cybercrime policymaking, investigation, prosecution and adjudication.

[1] International Telecommunication Union (2021, November 30) '2.9 billion people still offline: New data from ITU suggest 'COVID connectivity boost' – but world's poorest being left far behind' [press release]. https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

[2] Morgan, S. (2020, November 13) 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025'. *Cybercrime Magazine*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[3] Verizon (2022, May 24) 'Ransomware threat rises: Verizon 2022 Data Breach Investigations Report' [press release]. https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report

The *CCJ* contains scholarly articles, case studies and commentary by academics, policymakers, practitioners and experts exploring current issues in cybercrime and significant developments in the Commonwealth region. It will also better enable Commonwealth countries to develop sustainable digital economies.

The ITU estimates that, if supported by appropriate capacity building opportunities, 230 million 'digital jobs' in sub-Saharan Africa could generate an estimated US$120 billion in revenue by 2030. But these exciting prospects are threatened by many countries' vulnerability to cybersecurity attacks and cybercrime. Less than 60 per cent of Commonwealth countries have national cybersecurity strategic plans in place; only 18 per cent have ratified the Council of Europe's Budapest Convention, and an estimated 22 per cent have enacted mutual legal assistance (MLA) frameworks to facilitate international co-operation for transnational crimes. Given the transnational nature of cybercrime and the volatile nature of digital evidence, which necessitates real-time co-operation and cutting-edge technological skills, strengthened MLA frameworks are essential for the cyber-resilience of Commonwealth countries.

In this issue

This first issue of the *CCJ* examines contemporary issues and topics such as the use of artificial intelligence (AI) in judicial decision-making in criminal matters; co-dependency between cybercrime and organised crime; data privacy concerns in relation to bring-your-own-device (BYOD) working practices; a comparative review of national cybercrime laws; regional cyber-criminogenic theory; cybercrime reporting; and cyber diplomacy co-operation on cybercrime.

Dan Svantesson's article, 'Cybercrime and the Adoption of Artificial Intelligence Systems for Judicial Decision-Making in Criminal Justice Systems', recognises that there is a natural temptation to turn to AI to improve efficiencies and the rates of prosecution and adjudication of cybercrime. He notes, however, that since the criminal justice system is one of society's most sensitive functions, there is a need to proceed with extreme caution. The article provides guidelines on the adoption of AI systems for judicial decision-making in criminal justice systems, outlining current uses, perceived benefits, and the risks and challenges of AI systems in this context. It also makes recommendations regarding structural considerations that may serve to enhance co-operation and the sharing of knowledge.

Tim Hall and Ulrike Ziemer in their article, 'Cybercrime in Commonwealth West Africa and the Regional Cyber-Criminogenic Framework', explore a central conundrum of cybercrime: that despite being something that can be undertaken anywhere in the world with a connection to the internet, cybercrime tends to be disproportionately associated with a small number of Commonwealth countries. The article critically reviews the various literature that speak of these cybercrime geographies, and develops a framework that outlines the economic and social conditions that collectively identify as present within high cybercrime nations. The authors then apply this framework to Commonwealth West Africa and, finally, consider the lessons of their analysis for anti-cybercrime policy.

Mark Bryan Manantan's article, 'Cyber Diplomacy Co-operation on Cybercrime between Southeast Asia and Commonwealth Countries', advances the concept of peer-to-peer learning among states in the Global South. He does so by defying the conventional dyad of co-operation between developed and developing economies that is prevalent in the cyber diplomacy literature. This affords developing economies new pathways of collaboration to further reinforce their agency and autonomy. Given the shared contextual experiences of and mutual interests in combatting the increasing threats of cybercrime – and preserving regional and multilateral forums as neutral platforms, amid deepening strategic rivalry and the deterioration of global consensus on internet governance – Southeast Asian and Commonwealth countries can explore peer-to-peer learning as a viable alternative model of cyber diplomacy co-operation. Overall, the article's analysis and insights enrich the extant cyber diplomacy literature, while its policy recommendations promise to catalyse innovative, multi-stakeholder and cross-regional cyber capacity-building initiatives on cybercrime.

Juraj Sikra, Karen V. Renaud and Daniel R. Thomas in their article, 'UK Cybercrime Victims and Reporting: A Systematic Review' comprehensively analyse the problem of cybercrime victim underreporting in the United Kingdom. They argue that the reasons for underreporting cybercrime can be broken into three groups: types of cybercrime victims (individuals, private and public organisations); factors that affects victimhood (vulnerability, psychology, age, and research-driven models); and the realisation that improvements in cybercrime reporting are predominantly technical. The article makes the case that the latter factor ignores the social component of cybercrime, thereby failing to acknowledge the reporting-deterring side-effects of the UK's cyber responsibilisation agenda. The authors also make recommendations for how cybercrime reporting in the UK might be improved.

Brian Sang YK and Ivan Sang's article, 'A Comparative Review of Cybercrime Laws in Kenya', offers a critical review of Kenya's Cybercrimes Act by systematically comparing two international treaty instruments that influenced the drafting of the Act –the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection. The authors interrogate specific provisions of the Cybercrimes Act that are deemed inconsistent with international treaties and in-breach of Kenya's Constitution. The article recommends the amendment of these defective provisions to avoid the risk of interfering with digital rights and undermining the efficacy of Kenya's regime of cybercrime law.

Sophie Brain and Olajide Oyadeyi's article, 'Cybercrime and its Links to Organised Crime in the Caribbean', examines the relationship between organised crime and cybercrime in the Caribbean against the backdrop of the recent, explosive digital transformation experienced by the region. This, combined with low levels of cyber-resilience, have made the region an attractive target for cybercrime. The authors discuss how organised crime groups have exploited these vulnerabilities by taking advantage of the internet to perform illicit activities. The article highlights how the Caribbean region remains acutely unprepared to deal with cyberattacks and how, in several instances, the COVID-19 pandemic starkly exposed these weaknesses. The authors make recommendations on how this deficit can be curtailed.

Rotimi Ogunyemi and Akintunde Idowu's article, 'Data Security Concerns Raised by Bring-Your-Own-Device (BYOD) in Corporate Organisations' Hybrid and Remote Work Environments in Nigeria', examines both the benefits and drawbacks of BYOD in corporate organisations. The authors explore the legal and practical implications of BYOD policies in Nigeria, and assess the judiciary's approach to determining BYOD cases, by comparing case laws from various jurisdictions to establish the inconsistencies in the Nigerian legal framework. The article analyses data management and security practices associated with processing employees' personal data and provides cybersecurity policy recommendations for remote and hybrid work to balance the rights and interests of businesses, employees and other stakeholders.

The Commonwealth

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Cybercrime in Commonwealth West Africa and the Regional Cyber-Criminogenic Framework

Tim Hall[1] and Ulrike Ziemer[2]

Abstract

Cybercrime can, in theory, be carried out from anywhere in the world connected to the internet. Despite this, cybercrime displays markedly uneven patterns of perpetration across space. There is a nascent, multidisciplinary literature that has begun to engage with the questions of cybercrime's spatialities. This literature, at its heart, sees cybercrime as the product of the spatial co-presence of certain cyber-criminogenic combinations of conditions that occur unevenly across space. It advances versions of what we might call, 'a regional cyber-criminogenic thesis'. However, this literature remains relatively sparse, and its diversity has precluded any sustained cross-disciplinary dialogue from emerging. There is, for example, some discord within this literature around which combinations of conditions it identifies as potentially cyber-criminogenic, but, to date, no substantive cross-disciplinary scrutiny of these differences has emerged. This paper attempts to address this by articulating a regional cyber-criminogenic framework, accommodating perspectives from across this literature, which identifies eight potentially cyber-criminogenic conditions. The paper specifically considers the relevance of the regional cyber-criminogenic framework to Commonwealth nations. It includes an overview of cybercrime and the Commonwealth and then applies the framework to Ghana and Nigeria specifically, to examine the conditions that facilitate the development of cybercrime there. The paper also briefly considers the application of this framework to Commonwealth anti-cybercrime policy.

Keywords: cybercrime, regional, socio-economic, cyber-criminogenic, conditions, framework

[1] Department of Policing, Criminology and Forensics, University of Winchester (Winchester, UK).
[2] Department of Social Sciences, University of Winchester (Winchester, UK).

Introduction

Cybercrimes, of all kinds, are in theory placeless. They can be carried out from anywhere in the world with a connection to the internet. However, despite this, they display distinctive spatialities, characterised by markedly uneven patterns of perpetration across space. The literature, for example, identifies Eastern European and West African nations from which extensive economically motivated cyber frauds – such as advance-fee fraud and phishing – disproportionately originate, including the Commonwealth nations of Ghana and Nigeria (Ibrahim 2016a; 2016b; Kshetri 2013a; Lusthaus and Varese 2021). Elsewhere, the literature has associated extensive geopolitically motivated hacking with nations such as Russia and China, among others (Kshetri 2013a: 56; 2013b). It has also begun to recognise neighbourhood-level clusters of active cybercriminals in districts such as Ostroveni in the Romanian city of Râmnicu Vâlcea (Lusthaus and Varese 2021: 9) and Bijlmer in Amsterdam (Leukfeldt 2014; Loggen and Leukfeldt 2022). There are, of course, other spatialities of cybercrime, including those of victimisation (Halder 2021; Holt et al. 2018; Martellozzo and Jane 2017), policing, legislation and regulation (Gillespie 2019; Wall and Williams 2014), of the technical infrastructures that both sustain and defend against illegal online activities, and of awareness, education, and fear of cybercrime (Austin 2021; Cook et al. 2022). While these are equally deserving of critical scrutiny, this paper focuses specifically on the spatialities of cybercrime perpetration.

Acknowledging the spatialities of cybercrime perpetration (hereafter referred to simply as 'cybercrime') opens up the physical spaces within which cybercriminals are located, as well as the virtual spaces through which they operate, as legitimate sites of analysis (Lusthaus and Varese 2021). It raises empirical, theoretical and applied questions, namely:

- What are the specific spatialities of cybercrime?
- What regional, contextual conditions influence patterns of cybercrime offending?
- How might we mobilise these knowledges within anti-cybercrime policy and practice?

There is a nascent, multidisciplinary literature, spanning anthropology, criminology, sociology and investigative journalism; international relations and political economy; and statistics that has begun to engage with these questions. Despite their different disciplinary positions, these literatures, at their heart, all see cybercrime as the product of the spatial co-presence of certain cyber-criminogenic combinations of conditions that occur unevenly across space. They advance versions, then, of what we might call, 'a regional cyber-criminogenic thesis'. While this work has significantly advanced our understanding of the regional contexts from which cybercrime originates, we can recognise some limitations. Despite its recent growth, this literature remains relatively sparse (Perkins et al. 2022: 197), and its diversity has precluded any sustained cross-disciplinary dialogue from emerging. There is, for example, some discord between these literatures around which combinations of conditions they identify as potentially cyber-criminogenic, but to date no substantive cross-disciplinary scrutiny of, or reflection upon, these inter-disciplinary differences has emerged. There has only been one attempt to transcend these disciplinary positions and identify all potentially cyber-criminogenic conditions collectively articulated across this multidisciplinary literature (Hall et al. 2021) and we feel these findings demand some refinement. Therefore, despite only a limited history, this literature appears to be at something of an impasse with few spaces of cross-disciplinary contact evident.

This paper aims to exceed the rigidly disciplinary positions that have largely characterised work in this area to date, by articulating a regional cyber-criminogenic framework that accommodates perspectives from across the disciplinary span of this literature and which captures the full range of potentially cyber-criminogenic conditions it identifies. In doing so, it will critically examine the empirical foundations upon which the conditions included within this regional cyber-criminogenic framework rest, identifying areas where further research is needed. It will use this to articulate a space from which more cross-disciplinary, dialogic research agendas might emerge.

The paper specifically considers the relevance of this framework to Commonwealth nations and particularly those of West Africa. It includes an overview of cybercrime and the Commonwealth, exploring the implication of Commonwealth nations within the geographies of cybercrime perpetration and victimisation. It also explores the conditions that facilitate cybercrime originating in the West African Commonwealth nations of Ghana and Nigeria. The paper further considers the application of this framework in anti-cybercrime policy. Here, the paper draws upon lessons from successful information technology (IT) development in Rwanda, to suggest a policy direction that might contribute to mitigating the interaction of potentially cyber-criminogenic factors in Commonwealth countries such as Nigeria and Ghana with high incidents of cybercriminal activities.

Cybercrime

Cybercrime is a term that has been applied to a wide range of online crimes as diverse as fraud, blackmail, child pornography, revenge pornography, digital counterfeiting, cyber espionage and cyber terrorism. This empirical diversity ensures the term has little analytical currency and it is typical for research to focus on specific forms of cybercrime, rather than cybercrime generally. The literature is replete with attempts to define and classify cybercrime in various ways. These will not be rehearsed here but discussions of them are readily available (Neal 2010; Wall 2007; Yar 2019; Yar and Steinmetz 2019). In this paper, we draw on Ibrahim's (2016a) proposal for a tripartite taxonomy based on cybercriminals' motivations. This recognises socio-economic, psychosocial and geopolitical motivations (Table 1).

Table 1. Tripartite cybercrime framework

Socio-economic cybercrime	Psychosocial cybercrime	Geopolitical cybercrime
*Hackers and crackers	*Hackers and crackers	*Hackers – 'Hacktivist'
Cyber fraud	Child pornography	Cyber spies
Cyber embezzlement	Cyberstalking	Cyber espionage
Cyber piracy	Cyberbullying	**Cyber terrorism
Cyber blackmail	Revenge porn	Cyber vandalism
Romance scam	Cyber rape	Cyber assault
Online drug trafficking	*Cyber hate speech	*Cyber hate speech
*Cyber prostitution	*Cyber extortion	Cyber riot
*Cyber extortion	Obscenity	Cyber sabotage
Illegal online gambling	*Cyber prostitution	Cyber colonialism
*Cyber trespass	*Cyber trespass	Cyber rebellion
**Cyber terrorism	Cyber homicide	
	**Cyber terrorism	

Source: From Ibrahim 2016a, 45
Notes: *where the type of cybercrime appears in more than one column;
**where the type of cybercrime appears in more than two columns.

This taxonomy is not without its limitations. Its categories remain broad in the offences each includes and, as Table 1 demonstrates, some cybercrimes may have multiple motivations. However, it provides a useful heuristic device to frame discussions of the spatialities of cybercrime.

Cybercrime's spatial literatures

We can recognise three distinct research literatures that have explored the spatialities of cybercrime. These are now critically reviewed in turn.

Statistics

Statistical cybercrime literatures typically utilise national-level data, often analysing data for large groups of nations, and attempt to map the geographies of cybercrime at transnational/global scales (Kigerl 2012; 2016a; Lusthaus et al. 2020). They also encompass other aims, however, such as attempts to categorise cybercrime nation types (Kigerl 2016a) and to assess the impacts of legislation (Kigerl 2016b). These studies typically aim to first identify a dependent variable, a credible measure of the volume of cybercriminals active within nations or of cybercrime originating from different nations. This is not an unproblematic endeavour. Academic researchers are generally sceptical of cybersecurity industry reports (Kigerl 2012: 471; Lusthaus et al. 2020: 451–452) and are equally wary of cybercrime prosecution statistics, as these tend to be more reflective of differences in enforcement capacity and priority than levels of cybercriminal activity (Kigerl 2012: 474; Kshetri 2013a). Rather, data derived from spam archives are commonly used. Here, spam messages are extracted at volume and are geocoded through indicators of their origin, such as language or the originating internet protocol address (Kigerl 2012: 474). However, there are significant limitations inherent in these data sources that reflect the extent to which cybercriminals try to disguise their true locations (Kigerl 2016b: 67). At best, such data offer imperfect proxies of the locations of active cybercriminals and this remains a significant challenge for this literature.

Second, independent variables that may plausibly influence the volume of cybercrime originating from different nations are hypothesised and operationalised. Technological, economic and institutional variables, derived from publicly available global datasets produced by organisations such as the World Economic Forum and the World Bank, are the most widely deployed. This reflects the sparsity of robust national social and cultural datasets at the global scale. Examples of variables utilised include unemployment rate, internet users and participation in international anti-cybercrime legislation (Kigerl 2012) and computing resources, corruption, cybersecurity research and policy, and international relations (Mezzour et al. 2014). Finally, statistical procedures measure the effects of changes in the independent variable(s) on the dependent variable (cybercrime).

Theoretically, this literature draws primarily upon criminological traditions. The most widely deployed theory within this literature is routine activity theory (RAT). Originally developed to interpret volume crimes such as burglary, RAT interprets crime events as the product of the co-presence of motivated offenders and suitable targets, in the absence of capable guardians (Cohen and Felson 1979). It has interpreted cybercrime through motivated offenders (for example, due to a lack of legitimate economic opportunities for young people with IT skills) who operate within regional contexts who lack suitable guardianship (through legislative or institutional weakness or corruption), coming together with suitable targets (such as new or naïve internet uses) in online settings where technical defences are insufficient or can be easily circumvented (Holt et al. 2018; Kigerl 2012; Maimon et al. 2015; see also Leukfeldt and Yar 2016 for a wider review of the application of RAT to cybercrime).

This literature suggests that the most significant predictors of cybercrime activity within nations are gross domestic product (GDP) and internet users per capita. High-cybercrime nations, according to this literature, tend to be characterised by IT-literate populations, as suggested by higher rates of internet users per capita, in regional contexts where they are faced with limited opportunities to deploy their skills within the legitimate economy, as suggested by lower levels of GDP or high rates of unemployment (Kigerl 2012: 482). They tend to be associated with lower GDP only up to a point, however. Nations with very low levels of GDP tend to also be low-cybercrime nations, a reflection of their relative lack of technical infrastructure and IT literacy (Kigerl 2016a: 162). The significance of the interaction between poverty/a lack of economic opportunity and IT literacy has also been observed across other cybercrime literatures (Doyon-Martin 2015; Glenny 2008, 2011; Ibrahim 2016a, 2016b; Kshetri 2010; Lusthaus and Varese 2021). Other factors, such as high levels of corruption, have also been cited as additional predictors of cybercrime in some contexts (Mezzour et al. 2014).

International relations/political economy

A nascent international relations/political economy literature, of which Kshetri is the key author, offers broad surveys of cybercrime at the national and transnational scales, typically for nations widely perceived as major cybercrime threat nations such as China, Russia and Ukraine (Kshetri 2013a; 2013b) or for large groups of nations, such as the developing world (Kshetri 2010). It explores issues such as the nature of cybercrime within different nations and regions, comparative discussions of cybercrime, the ways in which cybercrime and cybersecurity increasingly shape the relations between nations, and national and regional responses to cybercrime (Kshetri 2010; 2013a; 2013b). It also commonly discusses the contextual conditions that underpin the development of cybercrime within different regions.

Table 2 summarises cyber-criminogenic conditions identified across Kshetri's analyses of cybercrime in China, the developing world, and the Former Soviet Union and Central and Eastern Europe (2009; 2010; 2013a; 2013b). These have been categorised using headings derived from RAT with the addition of one further category, 'facilitating context', to describe those conditions that contribute to cybercrime activities but do not fit into previously identified RAT categories. Although RAT is not a theory present within the international relations/political economy cybercrime literature, it provides a useful categorising device here. It is worth noting that some of the conditions below could, arguably, be allocated to more than one category or to alternative categories. 'High levels of corruption', for example, have been noted as a motivating factor within West African cybercrime (Adeniran 2011; Burrell 2008; Ibrahim 2016b; Tade 2013; Tade and Ibrahim 2011; Warner 2011).

Table 2. Cyber-criminogenic conditions identified within the international relations/political economy literature

Offender motivations
• Cybercriminals' confidence, a reflection of the low likelihood of being caught.
• Lack of legitimate economic opportunities, which generate economic motivations for cybercrime, especially for young people with IT skills.
• Wider social legitimacy and a lack of stigma associated with cybercrimes; 'hacking cultures'.
• Strongly nationalist political and cultural environments that encourage external victimisation and cyber wars.
Absence of capable guardians
• Permissive regulatory regimes.
• Limited capacity to fight cybercrime.
• Institutional weakness.
• High levels of corruption.
• Varying degrees of integration with the West in the realm of cybersecurity.
• Path-dependent externalities associated with cybercrime.
• Limited defences against cybercrime.
Suitable targets
• Widespread use of cheap, crime-prone hardware and software.
• Naïve, novice internet users with little awareness of cybersecurity products and practices.
• Presence of some highly digitised industries, such as China's online gaming industry, providing lucrative targets for cybercriminals.
Facilitating context
• Growing broadband connectivity.
• Presence of organised criminal groups involved in online, as well as offline, crime.

Source: Based on Kshetri 2009; 2010; 2013a; 2013b; Cohen and Felson 1979

A major contribution of this literature is that it recognises potentially cyber-criminogenic cultural and political conditions, beyond those predominantly technological, economic and institutional conditions identified within the statistical literature above. Specifically, it talks about the social legitimacy that cybercrime apparently enjoys in some regional contexts, including Eastern Europe, China and the global South, and the potential influence of strongly nationalist political contexts on cybercrime activity (Kshetri 2009: 143–144; 2013b: 52–53, 59). Of the former, with reference to China, Kshetri (2013b: 59) argues:

> *Recent studies and surveys have highlighted differences in culture associated with hacking in China and the West. For instance, many types of 'hackers' are considered to be socially undesirable in the West. The terms such as 'hacker' and 'hacking', on the other hand, seem to have somewhat more positive and less negative attitudes than they have acquired in the West.*

This literature also highlights the presence of stocks of suitable, domestic, targets in high-cybercrime nations, something that the statistical literature does not address.

Anthropology/criminology/sociology/investigative journalism

Anthropological, criminological and sociological studies of cybercrime, and accounts produced by the investigative journalist Glenny (2008; 2011), explore the grounded interactions between active cybercriminals within their regional contexts. These studies originate predominantly from two regions, Eastern Europe and the former Soviet Union, and West Africa, although there are some examples from beyond, including studies of cybercrime in Australia (Hutchings 2014), the Netherlands (Leukfeldt 2014), Germany, the UK and the USA (Leukfeldt et al. 2017), Turkey and Brazil (Glenny 2008; 2011). These studies are typically conducted at the micro scale, and employ ethnographic, interview, survey-based and archival methods. We can recognise a broad distinction between those studies that engage largely with official sources, through interviews and ethnographic encounters with law enforcement and criminal justice personnel, or analysis of court documents and police files (Beek 2016; Hutchings 2014; Leukfeldt 2014; Leukfeldt et al. 2017; Warner 2011), and those that engage largely with cybercriminals and/or members of their regional community through survey, interview and occasionally ethnographic methods (Adeniran 2011; Aransiola and Asindemade 2011; Armstrong 2011; Burrell 2008; Ibrahim 2016b; Lusthaus and Varese 2021; Ojedokun and Eraye 2012; Soudijn and Zegers 2012; Tade 2013; Tade and Ibrahim 2011; Voiskounsky et al. 2001). Studies that obtain direct interview testimony from active cybercriminals are relatively rare and are more common within a West African context (Aransiola and Asindemade 2011; Burrell 2008; Tade 2013; Tade and Ibrahim 2011). This reflects the greater accessibility of cybercriminals active within higher education student populations there. It is not uncommon to find studies of Nigerian cybercriminals conducted within universities, for example.

There is overlap with the cyber-criminogenic conditions identified within the statistical and international relations/political economy literatures discussed above and those articulated within these anthropological, criminological and sociological studies. For example, this literature, like the others discussed above, speaks of the presence of high levels of poverty among young people, interacting with technical literacy; political corruption; poor law enforcement capacity; and social contexts in which cybercrime is legitimised compared to other forms of criminal activity. However, by situating cybercrime within its complex regional cultural and geopolitical histories, this literature further extends recognition of the range of potentially cyber-criminogenic conditions. Specially, it talks of materialistic cultures that value wealth accumulation regardless of its origins (Adeniran 2011; Armstrong 2011; Ayodele et al. 2022; Glenny 2011; Ibrahim 2016a; Tade 2013; Tade and Ibrahim 2011) and regional histories of colonial or corporate exploitation that are deployed within justifications of Western victimisation (Armstrong 2011; Burrell 2008; Tade 2013; Warner 2011).

A regional cyber-criminogenic framework

This section applies the insights from the literature reviewed above into combinations of social, economic, political, technological and institutional conditions that might be regionally cyber-criminogenic. There has been one previous attempt to identify potentially cyber-criminogenic conditions collectively articulated across the multidisciplinary literatures discussed above (Hall et al. 2021). Here, 18 conditions ('factors') (plus four additional factors that were specific to West Africa) were identified. These spanned economic, social/cultural, technological, political, and legal/regulatory and policing factors. While valuable, we can recognise some limitations with this endeavour. First, a framework of 18–22 individual factors provides an unwieldy basis upon which to, for example, operationalise and conduct statistical analysis. Equally, it would be challenging for anthropological, criminological and sociological studies to respond to and accommodate the range of specific factors included within Hall et al.'s (2021) framework. A more refined framework, which retains the range that Hall et al. (2021) capture, while containing fewer categories, would offer a more user-friendly template. There is also some overlap between the factors identified in Hall et al. (2021). The authors, in identifying specific data sources to represent the 18 potentially cyber-criminogenic factors, collapse together two ('traditions of illicitness' and 'normative influence of the illicit within the cultural realm'), as they were too alike to meaningfully distinguish through statistical operationalisation (Hall et al. 2021: 289). There is additional potential overlap between other factors in this framework, such as 'high levels of corruption' and 'state and institutional weakness', for example. A framework consisting of broader categories would help to minimise or eliminate such overlap. In addition, Hall et al. (2021) do not recognise stocks of suitable domestic targets as a potentially cyber-criminogenic factor, despite this featuring in Kshetri's international relations/political economy analysis of cybercrime (2009; 2010; 2013a; 2013b). Recognising the application of RAT to cybercrime, noted earlier, we categorise the factors here through RAT categories, plus one additional category ('facilitating context') (see also Table 2 above).

Table 3. A regional cyber-criminogenic framework

Offender motivations

- An impoverished **legitimate economic context,** where opportunities in this economy do not match the skills levels of young people.
- A materialist **social/cultural context,** in which some forms of illicit wealth accumulation are legitimised.
- A corrupted **political context,** in which illicit wealth accumulation is legitimised.
- An antagonistic **geopolitical context,** in which external victimisation is legitimised.

Absence of capable guardians

- An inadequate **legal/regulatory and policing context,** in which cybercriminals have little chance of being prosecuted and convicted.

Suitable targets

- A vulnerable **socio-technological context** characterised by stocks of suitable domestic targets.

Facilitating context

- A developed **socio-technological context,** in which digital technologies are widely available and extensively used by the population.
- A developed **illicit economic context** characterised by extensive illicit and illegal economic markets and activities.

Source: Based on Hall et al. (2021)

The analysis underpinning this regional cyber-criminogenic framework is an attempt to transcend the rigidly disciplinary positions that have characterised research into the spatialities of cybercrime to date. It identifies a set of potentially cyber-criminogenic factors, based predominantly on analysis of socio-economic cybercrime, which have been collectively articulated across its multidisciplinary literatures. The regional cyber-criminogenic framework does not constitute a universal blueprint from which to read off the regional presence of cybercrime. Rather, it highlights factors that seem to have the potential to be cyber-criminogenic under certain circumstances. We should not, for example, assume that all the factors within the framework need to be present within a nation or region for cybercrime to develop extensively there. Future research, therefore, might focus on which combinations of factors within our framework are cyber-criminogenic, under what circumstances and in what regions. This would build upon suggestions in previous research (Hall et al. 2021: 293) that cyber-criminogenic combinations show some regional contingency.

Studies can confirm the presence of factors from the regional cyber-criminogenic framework within regions with recourse to a variety of forms of evidence. For some factors, for example, those relating to the legitimate economic and the political contexts, robust forms of objective and perception data are available, such as World Bank data on unemployment with advanced education[3] and Transparency International's annual Corruption Perception Index,[4] which are widely used in academic research. Some factors, however, which seem to lend legitimacy to the actions of cybercriminals in some contexts, derive from the sociocultural and geopolitical realms of regions. For these factors, data are more elusive. While we have some international survey data that include measures of the materialist orientations of different nations, for example, including the World Values Survey,[5] this is neither universal in its coverage nor particularly attuned to the question of the social legitimacy of illicit wealth accumulation. For this, we need to seek testimony from members of the regional community of high-cybercrime nations, explicitly exploring the question of the social legitimacy of cybercrime as a form of wealth accumulation within these settings. Further, in attributing causality to potentially cyber-criminogenic factors, the testimony of active or former cybercriminals, for example, in affirming their motivations, is a particularly valuable form of evidence.

Despite the value of the testimony of cybercriminals and members of their regional communities, their presence within cybercrime's literatures is somewhat patchy and uneven. Across all studies reviewed in this paper from all regions, the sum total of active or former cybercriminals who were interviewed, either directly by the authors of these studies or through secondary sources such as published interviews conducted by journalists, was 98. The majority of these were university students in West Africa, predominantly Nigeria, involved in cybercrime. In addition, approximately 1,200–1,400 members of the regional communities of high-cybercrime nations were surveyed within these studies. The empirical foundations of some factors identified within the regional cyber-criminogenic thesis, then, are somewhat restricted, show geographical bias and, in some cases, are now dated. Clearly, there is much that future research could do to generate more extensive testimony from active or former cybercriminals in these regions, and members of their regional communities.

The weight of literature informing this framework is uneven across different types of cybercrime. It primarily draws on literature exploring socio-economic and, to a smaller extent, geopolitical cybercrime. We might suppose that it will speak most directly to the geographies of these types of cybercrime, although this remains, for the moment, subject to empirical validation. No literature exploring psychosocial cybercrime informed the design of this framework; indeed, as noted at the head of this paper, very little literature exists that explores the spatialities of this type of cybercrime. Exploring and

[3] https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS

[4] https://www.transparency.org/en/cpi/2021

[5] https://www.worldvaluessurvey.org/wvs.jsp

interpreting the geographies of psychosocial cybercrime and building an equivalent framework relevant to crimes such as cyberbullying, cyberstalking and revenge porn, therefore, remains an endeavour for the future.

Cybercrime and the Commonwealth

Commonwealth nations are implicated in different ways into the global geographies of socio-economic cybercrime. While some are squarely identified as cybercrime threat nations, from which disproportionate amounts of cybercrime originate, others have been identified as, primarily, target nations, and/or those whose citizens display heightened levels of fear of cybercrime (Cook et al. 2022).

The evidence base currently available with which to sketch out the contours of cybercrime victimisation at the macro scale is somewhat restricted. Academic studies of socio-economic cybercrime victimisation at this scale are rare (Smirnova and Holt 2017). While cybersecurity industry analysis offers a variety of sources that speak to this issue, as noted above, researchers have urged caution in the use of such data (Kigerl 2012: 47; Lusthaus et al. 2020: 451–452). This limited evidence base reflects the challenges of obtaining accurate measures of cybercrime victimisation and the differences in patterns of victimisation associated with different types of socio-economic cybercrime.

Looking at cybersecurity industry sources, there is some consensus around which nations suffer the highest levels of cybercrime victimisation, whether this is measured by the number of victims, risk of encounter or by economic losses attributable to cybercrime (Federal Bureau of Investigation 2021; Lewis 2018; Statista no date). Notwithstanding the limitations of the evidence available, the primary driver of cybercrime victimisation at the macro scale, then, appears to be target suitability. There is some overlap between the nations identified in industry reports and those identified in the limited academic literature of socio-economic cybercrime victimisation at the macro scale. For example, Perkins et al.'s (2022) study of malicious spam distribution confirms the significance of target suitability, here measured in terms of being an Asian nation, GDP, political freedom and corruption. Smirnova and Holt's (2017: 1408) study of national victimisation patterns in stolen financial data markets also highlights the importance of risk minimisation.

While the USA is consistently identified as among the most victimised nations globally, the Commonwealth countries of Australia, Canada, India, New Zealand, South Africa and the UK are regularly identified as high-cybercrime victim nations within cybersecurity industry analysis. These countries all offer perpetrators extensive, digitally connected target populations, who, with the exceptions of India and South Africa, have relatively high GDPs per capita. As Lewis (2018: 7) argues: 'Unsurprisingly, the richer the country, the greater its loss to cybercrime is likely to be'. In addition to the USA, various academic studies identify Australia, Canada and the UK as Commonwealth cybercrime victim nations (Franklin et al. 2007; Holt et al. 2016; Holt and Lampke 2010, in Smirnova and Holt 2017: 1407).

Table 4. Commonwealth countries by K-means cluster assignment

Low-cybercrime countries	Advance-fee fraud specialists	Non-serious cybercrime countries	Phishing specialists
Bangladesh	Barbados	Brunei	Antigua and
Belize	Ghana	Canada	Barbuda
Botswana	Jamaica		Australia
Cameroon	Malaysia		Bahamas, The
Eswatini	Nigeria		Cyprus
Fiji	Samoa		Dominica
Gabon	Vanuatu		Grenada
Gambia, The			Guyana
India			Malta
Kenya			New Zealand
Kiribati			St Kitts and Nevis
Lesotho			Saint Lucia
Malawi			St Vincent and the Grenadines
Maldives			Seychelles
Mauritius			Singapore
Mozambique			Trinidad and Tobago
Namibia			United Kingdom
Pakistan			
Papua New Guinea			
Rwanda			
Sierra Leone			
Solomon Islands			
South Africa			
Sri Lanka			
Tanzania			
Togo			
Tonga			
Tuvalu			
Uganda			
Zambia			

Source: From Kigerl 2016a

Regarding cybercrime perpetration, Kigerl (2016a) conducted a statistical analysis that attempted to classify nations according to both the volume and type of their socio-economic cybercrime specialisation. Table 4 extracts all Commonwealth nations from this analysis.

This analysis suggests that many Commonwealth nations are either low-cybercrime or non-serious cybercrime countries. However, a number are classified as either advance-fee fraud or phishing specialists. Few of the nations identified in either of these two classifications (columns 2 and 4 in Table 4) has generated much attention within the literature of socio-economic cybercrime perpetration. Ghana and Nigeria are notable exceptions, with both the subject of extensive research literatures that have explored many dimensions of the cybercrime originating there. Ghana and Nigeria seem to represent the two apex cybercrime perpetration nations within the Commonwealth. Indeed, one of the most pervasive images of Nigeria within the international imagination is that of its notorious 419 email scams (Zook 2007). Multiple studies cited in the anthropological, criminological and sociological literatures reviewed above have confirmed West Africa as a high-cybercrime region. This association between Commonwealth West Africa and cybercrime undoubtedly causes significant reputational damage, with likely associated material consequences for this region. However, Kigerl's (2016a) analysis suggests that there are other Commonwealth nations that may be enrolled within the geographies of socio-economic cybercrime perpetration and are, therefore, worthy of scrutiny from a more geographically liberated research literature.

Cyber-criminogenic factors in Commonwealth West Africa

The extensive literature examining cybercrime in West Africa confirms the presence of factors from the regional cyber-criminogenic framework within this region. For example, it is common for studies conducted in both Ghana and Nigeria to highlight young people's frustration with their lack of opportunities due to West Africa's impoverished legitimate economic context, alongside a developed socio-technological context, evident through their relatively high levels of education and IT literacy, as motivations for their involvement in illegal online activities (Adeniran 2011; Aransiola and Asindemade 2011; Armstrong 2011; Ayodele et al. 2022; Burrell 2008; Ibrahim 2016a; Tade and Ibrahim 2011; Warner 2011). This issue is particularly acute in Nigeria, where in 2019, World Bank data identified the unemployment rate for Nigerians with advanced education as 17.15 per cent (World Bank 2023), the sixth highest globally. These widely held frustrations were also highlighted in, for example, Burrell's (2008) study of internet café culture in Ghana, which draws on multiple sources, including interview and ethnographic data:

> *It is not accurate to categorize these activities as arising out of a desire to 'gain something for nothing'. Instead, they appear to be informal attempts to realise personal gain by individuals who perceive legitimate channels of opportunity as being closed to them. This perspective was expressed among young people (not only Internet scammers) such as Stephen, an unemployed 21-year-old, who asserted that in Ghana, 'You can only get a job when you have a relative in that job. He will just link you to the money jobs. But if you don't know anybody there, just forget it, you're not getting any jobs'.*
>
> Burrell, 2008: 20

Young people's frustrations appear to be compounded by a materialist social/cultural regional context (Adeniran 2011; Armstrong 2011; Ibrahim 2016a; 2016b; Tade 2013; Tade and Ibrahim 2011). Although measuring materialism in the social and cultural realm is challenging, as are cross-cultural comparisons, empirical studies of cybercrime in West Africa frequently identify materialist orientations among young people as a contributory factor in the proliferation of West African cybercrime. Tade (2013: 697), for example, argues: 'The unbridled quest for materialism in Nigerian society has been argued as one of the factors influencing youth to innovate sinister ways of achieving success, without following the laid-down societal approved means'.

Numerous studies also identify a corrupted political context, which is seen to legitimise illicit wealth accumulation among cybercriminals and/or which directly facilitates it (Adeniran 2011; Burrell 2008; Ibrahim 2016b; Tade 2013; Tade and Ibrahim 2011; Warner 2011). These studies tend to identify the perception of illicit wealth generation among officials being deployed as a form of self-justification by those engaged in cybercrime. As one respondent, active in cybercrime, confirmed in Tade's (2013: 698) study, 'The issue of embezzlement is also germane. Monies given out to officials to create infrastructural facilities and even jobs to people are diverted into personal purse. This serves as negative influence on people, particularly the youths'. This view of West Africa as a region characterised by high levels of corruption is reflected in external data. Transparency International's Corruption Perception Index (2021)[6] ranks Ghana and Nigeria as the 73rd and 154th cleanest (least corrupt) nations in the world (out of a global total of 180).

Numerous studies of cybercrime in the region also identify an antagonistic geopolitical context that derives from the region's histories of colonial and corporate exploitation as a causal factor in the high rates of cybercrime originating from there (Armstrong 2011; Burrell 2008; Tade 2013; Warner 2011). This, like the perceptions of official corruption noted above, takes the form of cybercriminals deploying what they perceive as historical injustices as justification of their external victimisation. For example, Warner (2011: 747), argues:

[6] https://www.transparency.org/en/cpi/2021

> *Internationally,* Sakawa[7] *boys justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against Africans. Indeed, the histories of the Trans-Atlantic slave trade, combined with the none too-distant experience of colonialism and a surface-level adherence to the Pan-Africanist ideal of international social justice has combined to form a triumvirate of rationales to excuse the robbery of Westerners via the Internet.*

Or, as a practicing cybercriminal more succinctly put it on an internet forum: 'Sakawa in Ghana is pay back to the white men and woman…Have we all forget about what they done to as (us)' (Warner 2011: 747).

Several studies have highlighted an inadequate legal, regulatory and policing context to the problem of cybercrime in West Africa (Ayodele et al. 2022; Beek 2016). Beek's (2016: 309–310) study of cybercrime and policing in Ghana, for example, highlighted numerous challenges facing the policing response to cybercrime there. These included the inherent jurisdictional complexity of transnational cybercrime; a lack of specialist policing units, technical expertise and internet access; limited investigation of low-value cyber scams; a reliance on personal networks between the Ghanaian and international police forces for cases to be transferred to Ghana; and an expectation that foreign victims of cybercrime would travel to Ghana to seek justice. All of these suggest that cybercriminals, of the kinds noted in the West African literature, have only limited chances of getting caught and prosecuted for their activities.

The argument that cybercrime enjoys some degree of social legitimacy is also prominent within interpretations of West African cybercrime. Here, for example, it has been argued, based on qualitative interviews with 15 active cybercriminals in Nigeria, that cybercriminals here are viewed as less 'criminally minded' than those engaged in other forms of deviance (Ayodele et al. 2022: 32). Others cite the popularity of West African hip-hop music and films that justify the predatory actions of cybercriminals or paint them in a heroic light, as evidence of the wider legitimacy afforded to cybercrime in West African society (Lazarus 2018; Whitty 2018: 102–103). Studies that cite West African hip-hop music and films as evidence of the wider social legitimacy of cybercrime, however, offer no empirical evidence from members of the regional community to substantiate this claim, either directly within the studies themselves or indirectly through the sources they cite. For example, Whitty (2018) cites a textual analysis of popular *Sakawa* movies by a media studies scholar (Oduro-Frimpong, 2014), rather than any audience research or testimony from West Africans to confirm their consumption of these movies is consistent with a wider world view that regards cybercrime as socially legitimate. Interestingly, rather than offering uncritical portrayals of cybercriminals, the Ghanaian movies that Oduro-Frimpong analyses offer more nuanced portrayals that blend condemnation with acknowledgement of the motivations of cybercriminals. Oduro-

[7] *Sakawa* are spiritual practices sometimes used by cyberfraudsters in the belief that they will bring them success.

Frimpong argues, 'the films, while often acknowledging the role of greed in practitioners of *sakawa*, also foreground social problems such as joblessness and poverty' (2014: 143). Therefore, the social legitimacy of cybercrime is assumed from the popularity of these cultural products, rather than directly demonstrated.

It is worth considering the empirical evidence present in those anthropological, criminological and sociological studies of cybercrime that do survey or include testimony from members of the wider communities of Commonwealth West African high-cybercrime nations regarding the social legitimacy afforded to cybercrime in these contexts. Here, the evidence is somewhat patchy and indirect, as exploring this question is rarely a central aim of these studies. There is actually little evidence of this kind to directly endorse the social legitimacy argument present in studies of cybercrime conducted in West Africa. One respondent to a survey seeking parents' perspectives on Nigerian cybercrime did argue:

> *If a 419 boy [cybercriminal] is arrested, people would be sympathetic to him. They would ask, 'What type of crime has he committed? Is it just because he defrauded someone? Is it bigger than the ones people in government are committing? Why are they treating the small boy [cybercriminal] as if he has done something terrible?'*
>
> Ibrahim 2016b: 6

However, beyond this, evidence from the studies reviewed here, if anything, questions the validity of the social legitimacy thesis of cybercrime within a West African context. For example, Armstrong's (2011: 7) anthropological study of public discussions of *sakawa* in Ghana suggests that it, and associated cyber scams, are widely perceived in negative terms as un-Ghanaian and un-Christian. It is seen as 'Nigerian', and as a corrupting practice that has entered the country over Ghana's porous border with Nigeria. Further, Burrell's (2008) discussion of the practices and perceptions of internet scamming in Ghana reports examples of social condemnation of scammers by legitimate internet users there. Evidence is presented of concerns for the reputational damage internet scamming causes to Ghana's international image, as well as judgements of scammers as 'greedy or lazy' (2008: 24). She also notes concerns expressed by internet users in Ghana that they might fall victims to scams themselves and reports instances where Ghanaian interviewees had lost money to local (and international) scammers (see also Beek 2016: 317). Finally, Ojedokun and Eraye's (2012) study of the perceptions of Nigerian cybercriminals suggested they were regarded negatively by fellow students, who saw undergraduates engaged in cybercrime as extravagant and poorly performing academically.

This section, then, has demonstrated that while many of the factors within the regional cyber-criminogenic framework are undoubtedly present in Commonwealth West Africa, some questions remain regarding the claim that cybercrime enjoys widespread social legitimacy within this, and other, high-cybercrime regions. This points to one important avenue of further research.

Applying the regional cyber-criminogenic framework: tackling cybercrime in Commonwealth West Africa

This section considers how the regional cyber-criminogenic framework might inform policy designed to tackle cybercrime. Evidence would suggest that rather than simply the spatial co-presence of the factors identified in the framework, it is the *interactions* between them that are cyber-criminogenic. The interaction of IT literacy and regional poverty, for example, has emerged as particularly significant within statistical analysis of high-cybercrime nations (Kigerl 2012), and has been demonstrated in some settings within more ethnographic studies (Lusthaus and Varese 2021: 4). However, our own analysis suggests that the co-presence of these two factors is not universally cyber-criminogenic (Hall and Ziemer, 2023). Our research in the South Caucasus nation of Armenia reveals a country where many of the factors identified in the regional cyber-criminogenic framework are present, but where rates of socio-economic cybercrime perpetration remain low compared to nations with comparable profiles. Our interviews with a range of regional experts revealed that in Armenia, the interaction between IT literacy and regional poverty was mitigated to a large degree by a rapidly growing legitimate IT sector, partly driven by government policy over many years, partly by diaspora, and by international investment and relocations. Here, growth in this sector had been sufficient to absorb the pool of young people with IT skills in the country and wages were sufficiently high to deter illegality. This analysis highlights the potential geographical contingency of causality and suggests that cybercrime cannot simply be assumed from the spatial co-presence of certain factors within nations. It also indicates potential avenues of policy development. Therefore, what lessons might this case suggest for policies designed to tackle cybercrime in Commonwealth West Africa?

The Commonwealth East African nation of Rwanda, like Armenia, shares some characteristics identified within the cyber-criminogenic framework. For example, the proportion of the labour force with advanced education who were unemployed in Rwanda stood at 19 per cent in 2020. This was higher than the figures for both Ghana (4 per cent) and Nigeria (17 per cent).[8] Rwanda also scored and was ranked higher (score 2.8, rank 106) than Ghana (score 2.2, rank 125) and Nigeria (score 2.6, rank 113) on the infrastructure pillar of the World Economic Forum's *The Global Information Technology Report* (2016). This pillar compares electricity production, mobile network coverage, internet bandwidth and secure internet servers per million of the population for all nations. These data suggest potentially powerful cyber-criminogenic interactions in Rwanda.[9] However, despite this, at no point is Rwanda identified within the literature as a high-cybercrime nation. Indeed, Kigerl's (2016a) analysis (see Table 4) identifies Rwanda as a low-cybercrime nation. However, like Armenia, Rwanda has pursued a successful policy of

[8] https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS

[9] It should be noted, however, that Transparency International's (2021) *Corruption Perception Index*, records lower levels of corruption in Rwanda (ranked the 52nd 'cleanest' nation included in the index) compared to Ghana (ranked 73rd 'cleanest' nation) and Nigeria (ranked 154th 'cleanest' nation).

IT development in recent years (World Economic Forum 2022). Also in common with Armenia, this has taken place in the context of potentially cyber-criminogenic interactions in Rwanda. While these IT development policies have not been explicitly designed and promoted as anti-cybercrime measures, they offer another apparent example of IT development in the context of regional poverty and other cyber-criminogenic factors, without any obvious growth in indigenous cybercriminal activity. They also highlight an area that is worthy of further of attention in the context of cybercrime policy innovation, as well as in the context of economic development policy, within which it has primarily been discussed to date. There remains yet little literature on indigenous cybercrime in Rwanda and none that directly explores the relationships between IT development and cybercrime there. Addressing these lacunae in the literature would enhance our knowledge and understanding of cybercrime and the factors that drive its development – both within and beyond Rwanda. The case of IT development in Rwanda, then, offers a model that deserves greater scrutiny, not least for its potential transferability to other regional contexts and possibilities to mitigate cyber-criminogenic interactions.

Conclusions

This paper has shown that our understandings of the macro patterns of cybercrime perpetration and victimisation remain emergent, partial and in some cases, restricted. This is the case both globally and with specific regard to Commonwealth nations. Kigerl's (2016a) analysis (Table 4), for example, revealed several Commonwealth nations that potentially contain extensive cybercrime activity, about which its literatures have said almost nothing to date. There is a clear geographical bias towards the former Soviet Union, Eastern Europe, West Africa and, to an extent, China, in the existing cybercrime research. We would recommend future research range beyond these 'usual suspects' to other regions highlighted as potentially cyber-criminogenic by this, and other, analysis. A more comprehensive analysis of cybercrime within all Commonwealth nations would contribute significantly to our knowledge here. We would also advocate that future research be more interdisciplinary and dialogic. For example, our regional cyber-criminogenic framework might inform the factors included in future statistical analysis of cybercrime. This analysis is valuable in producing maps of potentially high-cybercrime nations through factor correlations. However, determining causation requires more grounded, field-based research. Statistical analysis, therefore, might profitably guide these more grounded, ethnographically informed research endeavours.

There is also scope for future research to engage more critically with the theoretical frameworks that have been deployed within the literatures reviewed here. RAT, for example, has now been quite extensively used to interpret the regional presence of cybercrime. At the same time, the literatures reviewed above have identified the interactions between regional poverty and IT literacy to be particularly cyber-criminogenic. However, in RAT terms this combination alone does not include a factor related to the absence of capable guardians, one of the triad of conditions that RAT argues is necessary for a crime event to occur. This suggests that either this analysis has failed to identify factors related to the regional absence of capable guardians, or, alternatively, that RAT, in being applied to cybercrime, requires some modification. Our analysis also suggests the addition of another factor, 'facilitating context', beyond the original RAT triad. Future research might ask, then, whether factors from all RAT categories are required to be present within cyber-criminogenic regions.

Our analysis has also revealed that the literature has collected only limited direct testimony from active or former cybercriminals, valuable in determining offender motivations, and relatively little testimony from members of their regional communities, valuable in addressing the question of whether cybercrime enjoys social legitimacy within some regional contexts. Although an issue not restricted to the literature of West Africa, more robustly addressing such lacunae in a Commonwealth West African context would offer significant empirical contributions to the cybercrime literature.

The most pressing issue facing Commonwealth nations, revealed by this review of the literatures of cybercrime, is addressing the high rates of socio-economic cybercrime originating in Ghana and Nigeria. As the case of Armenia above shows, potentially cyber-criminogenic combinations of factors may be present within nations, but rates of cybercrime may remain low where there are other factors present, such as Armenia's rapidly growing IT sector, that mitigate their interaction. This suggests that exploring such mitigating factors in different regional contexts might offer new paths of anti-cybercrime policy innovation. Therefore, a cybercrime policy priority for the Commonwealth to pursue, might be to consider the transferability of policies of IT development, such as those pursued in Rwanda, to a West African context, and to explore their potential to mitigate cyber-criminogenic interactions, particularly between economic poverty and socio-technological literacy, which have been identified in Ghana and Nigeria.

References

Adeniran, A (2011), 'Cafe culture and heresy in Yahooboyism in Nigeria', in K Jaishankar (Ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*, CRC Press, Abingdon, 3–12.

Armstrong, A, (2011), '"Sakawa" Rumours: Occult Internet Fraud and Ghanaian Identity', UCL Anthropology Working Papers Series, Working Paper No. 08/2011, University College London.

Aransiola, JO, and SO Asindemade (2011), 'Understanding cybercrime perpetrators and the strategies they employ in Nigeria', *Cyberpsychology Behavior and Social Networking*, Vol. 14 No. 2, 759–763.

Austin, G (Ed.) (2021), *Cyber Security Education: Principles and Policies*, Routledge, Abingdon.

Ayodele, A, J Kehinde Oyedeji and H Olamide Badmos (2022) 'Social construction of internet fraud as innovation amongst youths in Nigeria', *International Journal of Cybersecurity Intelligence and Cybercrime*, Vol. 5 No. 1, 23–42.

Beek, J (2016), 'Cybercrime, police work and storytelling in West Africa', *Africa*, Vol. 86 No. 2, 305–323.

Burrell, J (2008), 'Problematic empowerment: West African internet scams as strategic misrepresentation', *Information Technology and International Development*, Vol. 4 No. 4, 15–30.

Cohen, LE, and M Felson (1979), 'Social change and crime rate trends: a routine activity approach', *American Sociological Review*, Vol. 44 No. 4, 588–608.

Cook, S, L Giommoni, N Trajtenberg Pareja, M Levi and ML Williams (2022), 'Fear of economic cybercrime across Europe: a multilevel application of routine activity theory', *British Journal of Criminology*, available at: 10.1093/bjc/azac021.

Doyon-Martin, J (2015), 'Cybercrime in West Africa as a result of transboundary e-waste', *Journal of Applied Security Research*, Vol. 10 No. 2, 207–220.

Federal Bureau of Investigation (2021) *Internet Crime Report 2021*, Internet Crime Complaint Centre, Washington, DC.

Franklin, J, V Paxson, A Perrig and S Savage (2007), 'An inquiry into the nature and causes of the wealth of Internet miscreants', in ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, 275–288.

Gillespie, AA (2019), *Cybercrime: Key Issues and Debates*, second edition, Routledge, Abingdon.

Glenny, M (2008), *McMafia: Crime Without Frontiers*, Bodley Head, London.

Glenny, M (2011), *Dark Market: Cyberthieves, Cybercops and You*, Bodley Head, London.

Halder, D (2021), *Cyber Victimology: Decoding Cyber-Crime Victimisation*, Routledge, Abingdon.

Hall, T, B Sanders, M Bah, O King and E Wigley (2021), 'Economic geographies of the illegal: the multiscalar production of cybercrime', *Trends in Organized Crime*, Vol. 24 No. 2, 282–307.

Hall, T and U Ziemer (2023), *Exploring the Relationship Between IT Development, Poverty and Cybercrime: An Armenia Case Study,* in press.

Holt, TJ, GW Burruss and AM Bossler (2018), 'Assessing the macro-level correlates of malware infections using a routine activities framework', *International Journal of Offender Therapy and Comparative Criminology*, Vol. 62 No. 6, 1720–1741.

Holt, TJ, and E Lampke (2010), 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies*, Vol. 23 No. 1, 33–50.

Holt, TJ, O Smirnova and YT Chua (2016), 'Exploring and estimating the revenues and profits of participants in stolen data markets', *Deviant Behavior*, Vol. 37 No. 4, 353–367.

Hutchings, A (2014), 'Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission', *Crime Law and Social Change*, Vol. 62 No. 1, 1–20.

Ibrahim, S (2016a), 'Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals', *International Journal of Law, Crime and Justice*, Vol. 47, 44–57.

Ibrahim, S (2016b), 'Causes of socioeconomic cybercrime in Nigeria', *Proceedings of 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, available at: https://ieeexplore.ieee.org/document/7740439.

Kigerl, A (2012), 'Routine activity theory and the determinants of high cybercrime countries', *Social Science Computer Review*, Vol. 30 No. 4, 470–486.

Kigerl, A (2016a), 'Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates', *International Journal of Cyber Criminology*, Vol. 10 No. 2, 147–169.

Kigerl, A (2016b), 'Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction?', *Trends in Organized Crime*, Vol. 21 No. 1, 62–78.

Kshetri, N (2009), 'Positive externality, increasing returns and the rise in cybercrimes', *Communications of the ACM*, Vol. 52 No. 12, 141–144.

Kshetri, N (2010), 'Diffusion and effects of cyber-crime in developing economies', *Third World Quarterly*, Vol. 31 No. 7, 1057–1079.

Kshetri, N (2013a), 'Cybercrimes in the former Soviet Union and central and Eastern Europe: current status and key drivers', *Crime, Law and Social Change*, Vol. 60 No. 1, 39–65.

Kshetri, N (2013b), 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research*, Vol. 13 No. 1, 41–69.

Lazarus, S (2018), 'Birds of a feather flock together: the Nigerian cyber fraudsters (yahoo boys) and hip hop artists', *Criminology Crime Justice Law and Society*, Vol. 19 No. 2, 63–81.

Leukfeldt, ER (2014), 'Cybercrime and social ties: phishing in Amsterdam', *Trends in Organized Crime*, Vol. 17 No. 4, 231–249.

Leukfeldt, ER and M Yar (2016), 'Applying routine activity theory to cybercrime: a theoretical and empirical analysis', *Deviant Behaviour*, Vol. 37 No. 3, 263–280.

Leukfeldt, ER, Kleemans, ER and WP Stol (2017), 'Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis', *Crime, Law and Social Change*, Vol. 67 No 1, 39-53.

Lewis, J (2018) *Economic Impact of Cybercrime – No Slowing Down*, CSIS, Santa Clara, CA.

Loggen, J and R Leukfeldt (2022), 'Unravelling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands', *Trends in Organized Crime*, Vol. 25 No. 2, 205–225.

Lusthaus, J, M Bruce and N Phair (2020), 'Mapping the geography of cybercrime: a review of indices of digital offending by country', *IEEE European Symposium on Security and Privacy Workshops (Euro SandPW)*, 448–453.

Lusthaus, J and F Varese (2021), 'Offline and local: the hidden face of cybercrime', *Policing: A Journal of Policy and Practice*, Vol. 15 No. 1, 4–14.

Maimon, D, T Wilson, W Ren and B Berenblum, B (2015), 'On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents', *British Journal of Criminology*, Vol. 55 No. 3, 615–634.

Martellozzo, E and EA Jane (Eds.) (2017), *Cybercrime and Its Victims*, Routledge, Abingdon.

Mezzour, GL, R Carley and KM Carley (2014), *Global Mapping of Cyber Attacks*, Carnegie Mellon University.

Neal, S (2010), 'Cybercrime, transgression and virtual environments', in J Muncie, D Talbot and R Walters (Eds.) *Crime: Local and Global*, Willan, Devon.

Oduro-Frimpong, J (2014), '*Sakawa* rituals and cyberfraud in Ghanaian popular video movies', *African Studies Review*, Vol. 57 No. 2, 131–14.

Ojedokun, UA and MC Eraye (2012), 'Socioeconomic lifestyles of the yahoo boys: a study of perceptions of university students in Nigeria', *International Journal of Cyber Criminology*, Vol. 6 No. 2, 1001–1013.

Perkins, RC, J Howell, CE Dodge, GW Burruss and D Maimon (2022), 'Malicious spam distribution: a routine activities approach', *Deviant Behavior*, Vol. 43 No. 2, 196–212.

Smirnova, O and TJ Holt (2017), 'Examining the geographic distribution of victim nations in stolen data markets', *American Behavioral Scientist*, Vol. 61, No. 11, 1403–1426.

Soudijn, MR and BCHT Zegers (2012), 'Cybercrime and virtual offender convergence settings', *Trends in Organised Crime*, Vol. 15 No. 2–3, 111–129.

Statista (no date) 'Percentage of internet users in selected countries who have ever experienced any cyber crime from November to December 2021', Cyber threat encounter rate by country 2021, Statista, available at: https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/ (accessed 27 September 2022).

Tade, O (2013), 'A spiritual dimension to cybercrime in Nigeria: the "yahoo plus" phenomenon', *Human Affairs*, Vol. 23 No. 4, 689–705.

Tade, O and A Ibrahim (2011), 'Social organization of internet fraud among university undergraduates in Nigeria', *International Journal of Cyber Criminology*, Vol. 5 No. 2, 860–875.

Transparency International (2021) *Corruption Perception Index 2021*, Transparency International, Berlin, available at: https://www.transparency.org/en/cpi/2021 (accessed 24 January 2023).

Voiskounsky, AE, JD Babaeva and OV Smyslova (2000), 'Attitudes towards computer hacking in Russia', in BD Loader and D Thomas (Eds.) *Cybercrime: Security and Surveillance in the Information Age*, Routledge, Abingdon, 56–84.

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

Wall, D and M Williams (Eds.) (2014), *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, Routledge, Abingdon.

Warner, J (2011), 'Understanding cyber-crime in Ghana: a view from below', *International Journal of Cyber Criminology*, Vol. 5 No. 1, 736–749.

Whitty, MT (2018), '419 – it's just a game: pathways to cyber-fraud criminality emanating from West Africa', *International Journal of Cyber Criminology*, Vol. 12 No. 1, 97–114.

World Bank (2023), 'Unemployment with advance education (% of total labour force with advanced education)', World Bank, available at: https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS (accessed 24 January 2023).

World Economic Forum (2016), *The Global Information Technology Report 2016*, World Economic Forum, Geneva.

World Economic Forum (2022), 'Rwanda is tackling digital development challenges – and succeeding', World Economic Forum, available at: https://www.weforum.org/agenda/2022/07/rwanda-is-tackling-digital-development-challenges-and-succeeding/ (accessed 14 September 2022).

Yar, M (2019), 'Transnational governance and cybercrime control: dilemmas, developments and emerging research agendas', in T Hall and V Scalia (Eds.) *A Research Agenda for Global Crime*, Edward Elgar, Cheltenham, 91–106.

Yar, M and KF Steinmetz (2019), *Cybercrime and Society*, third edition, Sage, London.

Zook, MA (2007), 'Your urgent assistance is requested: the intersection of 419 spam and new networks of imagination', *Ethics, Place and Environment,* Vol. 10 No. 1, 65–88

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

The Commonwealth

UK Cybercrime, Victims and Reporting: A Systematic Review

Juraj Sikra,[1,2,3] Karen V. Renaud[1,4,5,6] and Daniel R. Thomas[1,7]

Abstract

Individuals and organisations based in the UK often fall foul of cybercriminals. Unfortunately, however, these kinds of crimes are underreported [68][123][133]. This underreporting hampers the ability of crime-fighting units to gauge the full extent of the problem, as well as their ability to pursue and apprehend cybercriminals [14][81].

To comprehend cybercrime underreporting, we need to explore the nature of UK cybercrime and its impact on UK-based victims. We investigated the entire landscape by carrying out a systematic literature review, covering both academic and grey literature. This review sought to answer three research questions.

1. What characterises cybercrime in the UK?
2. What is known about UK cybercrime victims?
3. What influences and deters cybercrime reporting in the UK?

Our investigation revealed three types of reportable cybercrime, depending on the target: individuals, private organisations and public organisations.

Victimhood varies depending on a number of identified dimensions, including vulnerability aspects, psychological perspectives, age-related differences and researcher attempts to model the victims of cybercrime. We also explored UK victims' reported experiences in dealing with the consequences of falling victim to a cybercrime.

In terms of cybercrime reporting, we identified three kinds of reporting: human-to-human, human-to-machine and machine-to-machine. In examining factors deterring reporting, we incorporated discussions of policing, and the challenges UK police forces face in coping with this relatively novel crime. Unlike in traditional

[1] Computer and Information Sciences, University of Strathclyde (Glasgow, UK).
[2] Faculty of Psychology, Taras Shevchenko National University of Kyiv (Kyiv, Ukraine).
[3] E-mail: juraj.sikra@strath.ac.uk
[4] Department of Information Systems, Rhodes University (Grahamstown, South Africa).
[5] School of Computing, University of South Africa (Pretoria, South Africa).
[6] Division of Cybersecurity, Abertay University (Dundee, UK).
[7] Computer Laboratory, University of Cambridge (Cambridge, UK).

crimes, perpetrators possess sophisticated technological skills and may reside outside of the UK's police jurisdiction. We discovered a strong social dimension to reporting incidence, with the UK government's cyber-responsibilisation agenda likely playing a major role in deterring reporting. This strategy involves the government providing a great deal of advice and then expecting citizens to take care of their own cybersecurity. Within this, if citizens do not act on the advice, they have to accept the consequences.

Improvements in cybercrime reporting have to date been technologically focused. This neglects the social dimensions of cybercrime victimhood and does not acknowledge the reporting-deterring side-effects of the UK's cyber-responsibilisation agenda. We thus conclude with suggestions for improving cybercrime reporting in the UK.

1. Introduction

Cybercrime is a reality of everyone's networked lives, and UK citizens are no exception, and are increasingly falling victim [52][60][105][113]. Indeed, Caneppele, and Aebi [24] report that between a third and half of the crimes committed in a country are likely to be cybercrimes. Cybercrime costs citizens and the UK dearly, as shown in Figure A1 in the Appendix. The consequences of falling victim to a cybercrime can be significant and are not limited to financial loss. Some victims suffer from poor mental health and other health consequences [102]. The UK's cybercrime landscape is poorly understood, given that cybercrimes are significantly underreported [68][105][123][133]. Such underreporting makes it difficult for law enforcement to gauge the true extent of cybercrime [116] or to invest resources appropriately to address it [14][81].

One aspect that could be deterring reporting is the cyber-responsibilisation agenda pursued by the UK government, in common with other neoliberal governments [118][119]. Responsibilised citizens are given advice and then are expected to embrace the responsibility and accept the consequences if they do not follow it. Consequently, victims may be too embarrassed to report what has occurred if they did not, or could not, follow the government-issued advice [1]. Reporting a cybercrime may well be considered an embarrassing admission of negligence and signal irresponsibility. As such, reporting could trigger an additional trauma that victims may dread.

This paper focuses only on the UK because carrying out this kind of study globally would introduce noise emanating from a large variety of legal, economic and policing differences, and this might confound our analysis and obscure insights. Fortunately, UK findings related to underreporting can still offer lessons for other countries, especially those with neoliberal governments, given that a side-effect of responsibilisation may be to deter reporting.

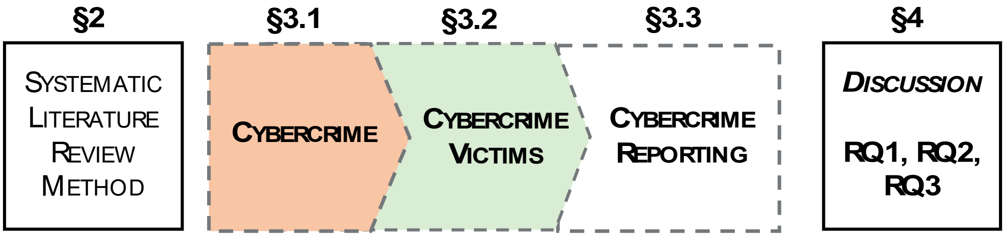
A systematic review was carried out to answer the following research questions with respect to the UK's cybercrime landscape:

RQ1: What characterises cybercrime in the UK?

RQ2: What is known about UK cybercrime victims?

RQ3: What influences and deters cybercrime reporting in the UK?

Figure 1. Structure of the paper: Cybercrime, Victims and Reporting in the UK



As Figure 1 shows, Section 2 outlines the systematic literature review methodology. Section 3 then reports our findings on UK cybercrime (Section 3.1), UK cybercrime victims (Section 3.2) and cybercrime reporting (Section 3.3). Section 4 returns to the research questions and discusses the findings. Section 5 concludes.

2. Systematic literature review methodology

Using the principles of systematic research as outlined by Pickering et al. [112], a search was conducted across the following databases: Scopus, Web of Science and ProQuest. Keywords were chosen to meet the needs of each of the research questions. The search period commenced in 1999, based on publicly available information concerning the growth of online retail in the world, which saw its inception in the mid-1990s onward [93]. The earliest included article concerning the subject is by Fisher in 2008 [51]. The searches are depicted using the PRISMA diagrams supplied in the Appendix. Table 1 maps the research questions to the PRISMA diagrams.

Table 1. Systematic review process

	PRISMA in Appendix
RQ1: What characterises cybercrime in the UK?	Figure A2
RQ2: What is known about UK cybercrime victims?	Figure A3
RQ3: What influences and deters cybercrime reporting in the UK	Figure A4

We focused primarily on UK sources but included publications from outside of the UK where we considered that the applicability of their findings to the UK could be argued. Where we found research from other countries that offered lessons to the UK, we retained these. Table A1 in the Appendix provides a list of these references.

Filtering

The documents were filtered based on their titles and abstracts, which were the core determinants for including them in the review. Documents that were included in the review were grouped according to common themes.

Analysis

The approach applied within was adapted from Robinson's guidance on thematic analysis [120]. Specifically, an inductive approach was operationalised, which commences with data immersion (i.e., re-reading the identified articles) and results in several emergent themes. These themes are then contrasted against all the data to ensure a good fit.

3. Results

Previous research has shown that cybercriminals seek to understand victims in a predatory way so that they can insert themselves into their lives by exploiting their needs [17][43][66][89][106][140]. Johnson [74] reports that 20 per cent of UK survey respondents had found malicious software on their devices over the past three years. This demonstrates a measure of success in compromising UK citizens' devices. We now consider what is reported about UK-related cybercrime.

3.1 Cybercrime in the UK

The National Crime Agency (NCA) estimated that 1 million cybercrimes were committed in 1999 across the UK's households [105]. Similarly to in other countries, there is evidence that the number of cyber-offences is increasing: by 2021 it had doubled, to 1.8 million, relative to 2019 [50]. In December 2021 [130], it was reported that 48 per cent of UK citizens had experienced cybercrime, as compared with 76 per cent of Indians and only 32 per cent of Japanese. According to Daniel Markuson [99], cybercriminals, like other criminals, look for opportunities. Countries where citizens spend more time online, and shop more online, are more at risk. The top 10 'at risk' countries include the UK.

Fraud was the most common type of cybercrime targeting UK citizens in the NCA survey in 2019 [105], with Internet-enabled fraud making up 54 per cent of all fraud cases. Romance fraud was another major type of crime, causing economic damage of £60 million, primarily targeting women with disposable funds.

A major source of cybercrime incidents in the UK (by number) is illegal booter services, which allow criminals to target specific organisations with denial-of-service attacks. In 2016, a 20-year-old British male was sentenced to 18 months in a youth detention centre and required to pay £800 damages for running four booter services [31].

In the UK, criminal networks are often responsible for attacks [83]. The NCA survey found that that Russian-language cybercrime groups posed the greatest threat to the UK [105]. Yet, Lavorgna [83] has warned against overestimating the extent of organised cybercrime within the UK lest public funds be unnecessarily depleted, because cybercriminals are not all affiliated with organised groups. Another common kind of crime that targets UK citizens is romance scams, which involve interaction with a fake profile [140]. People are tricked into sending money to these scammers in exchange for explicit media [66][107].

Research tracing individual cybercrime reports to offenders has revealed interesting results [17]. It emerges that a relatively small number of offenders are responsible for many offences. A deeper analysis of these reported results reveals that the offenders who attract the most reports are not always those who make the most money from their crimes.

In May 2022, the Director of the UK's Government Communications Headquarters (GCHQ), Sir Jeremy Fleming, advised the public about the organisation's proactive approach to cyber-fraud, which had spiked in conjunction with Russia's illegal invasion of Ukraine. Specifically, GCHQ took down 2.7 million online scams during 2021 alone [52]. He argued that this approach mirrored the overall restructuring of the western security architecture, as summarised by the old Latin proverb: *si vis pacem, para bellum* – that is, 'If you want peace, prepare for war.'

Typology of cybercrime

A three-dimensional typology of cybercrime emerged from the literature, reflecting attacks against (1) individuals, (2) private institutions and (3) public institutions. According to Levi [88], companies rather than individuals incur the largest financial losses. Yet the impact on individuals should not be downplayed, as they are likely to be seen as easy targets for cybercriminals [128]. The typology is critical for improving cybercrime reporting because it supports categorisation and coding of offences.

Even so, it should be noted that an attack on an individual can spread to their employer's devices. A case in point occurred in Scotland in March 2022 [75], when the Scottish Association for Mental Health experienced a ransomware attack that sprang from an individual employee's personal device. This resulted in passports and personal data being made public.

Cybercrime against individuals: In 2016, Levi [87] references a cybercrime survey of 3.8 million cases. He found that individuals were most likely to experience bank card fraud. The total number of incidents of fraud in 2016 exceeded 2.5 million (66 per cent of all incidents). Online shopping fraud totalled more than 1 million incidents (28 per cent of all incidents). Other authors highlight denial-of-service attacks on end users (i.e., game players) [31]. Shared computers constitute a particular problem given the ease with which users' personal details can be collected and sold [3] and with which compromises can jump from one individual's device to another's and from individual to organisational devices.

Kemp et al. [79] analysed the changes in cybercrime during the pandemic in the UK. They found a significant increase from over 2,000 reported offences before lockdown to nearly 4,000 offences during lockdown. Kemp et al. found that the closing of physical shops led to an increase in online shopping, which sometimes resulted in fraud. On the other hand, a reduction in ticket-related leisure activities and aviation reduced ticket-related fraud. Cybercriminals exhibit adaptiveness and innovativeness.

Cybercrime against private institutions: The 2022 Cyber Security Breaches Survey [47] reported that 39 per cent of UK businesses were attacked in 2022, mostly by phishing attempts (83 per cent). In the past, these have included attacks on banks via forged cheques [51]. Cybercriminals can also impersonate a CEO's email, to achieve a speedy transfer of funds to a named 'supplier' (known as 'CEO fraud' or 'business email compromise' [91]. Small and medium-sized enterprises (SMEs) are particularly vulnerable to these kinds of attacks [90]. However, Kemp et al. [79] found that, during the pandemic, organisations experienced decreased levels of cybercrime. The suggested explanations relate to the closing of businesses and restructuring, which may have reduced attack surface and victimhood.

Cybercrime against public institutions: Wirth [143] outlined the devastating effect of the WannaCry ransomware on the National Health Service (NHS) in 2017. WannaCry impacted 81 of 236 hospital trusts and 597 of 7,545 GP surgeries and resulted in the cancellation of 20,000 appointments. This sets these kinds of targeted cybercrime apart from other kinds of crime [39]. Criminals who burglarise or mug would not be able to attack this many targets simultaneously. A single cyber-attack can target multiple organisations and be hard to recover from, given the required technological expertise [5]. WannaCry 2017 is a case in point [106].

Summary

The UK is clearly experiencing high levels of cybercrime. The profile is not identical to that in other EU countries [116]. For example, online shopping fraud affects 0.6–4 per cent of people annually based on a comparison of survey data vs police data, and the UK's higher online shopping levels will mean that it is more affected than other countries where there is less shopping online. Online banking fraud, too, is less common in the EU than in the UK, at around 1–2 per cent. Less than 1 per cent of the EU population have been victimised via advance fee fraud or identity fraud. Cybercriminal creativity and adaptivity target victims where the attack surface presents itself. With so many UK residents being online, the attack surface is large enough to facilitate attacks.

The next section considers UK cybercrime victims.

3.2 UK cybercrime victims

Action Fraud has highlighted a dramatic spike in cybercrime against individuals during the recent COVID-19 pandemic [17], so it is reasonable to argue that cyber-victimhood is increasing. How does the UK government respond? In 2008, Shadow Home Secretary David Davis MP, after his own victimisation, criticised the UK government for being ineffective in tackling cybercrime [63]. Hunter [63] critiqued the lack of a dedicated centre for tackling cybercrime and the police's tendency to investigate only high-value crimes. At that point, Action Fraud, a designated centre for cybercrime reporting, was established. However, the problem with investigating only high-value offences persists. The difference is that Hunter complained that the police investigated only losses of more than £500. In 2019, that figure increased to losses over £100,000 [35]. The literature also highlights the cost of an effective defence system to assist victims [11].

Böhme [11] argues that cyber-attacks must be quantified in terms of both financial and psychological damage but also acknowledges that it is difficult to quantify such attacks in terms of the latter. However, it is important to recognise both kinds of impact in terms of delineating the cybercrime landscape.

Victims can experience adverse health consequences. Button et al. [22] found that some cyber-victims experienced headaches, flare-ups of existing conditions such as fibromyalgia and Crohn's disease, withdrawal from relationships, isolation, depression, anxiety and suicide. Other research from UK psychiatry argues that, while it is difficult to develop an objective compensation for psychological distress, the affected party should be provided with psychological therapy to help them deal with the victimhood trauma [13].

Böhme and Moore [23] analysed the experiences of victims within the EU (which included the UK at the time of the study). They found that victims reduced their online shopping and online banking activities by 4–5 per cent. Moreover, people who had been exposed to information about cybercrime threats were twice as likely to diminish their online activity, as compared with actual victims, suggesting that dread and fear were preventing them from benefiting from the online world. Indeed, Cross et al. [44] revealed unrealistic risk perceptions, with respondents considering their risk of victimisation to be low despite most having reported falling victim to a cybercrime in the past. Considering these two studies, it seems that those who have fallen victim to cybercrime underestimate the risk, whereas those who merely hear about the possibility of falling victim deliberately reduce their risk by changing their behaviours.

Individual victim profiles

There are several dimensions to consider here.

Vulnerability: Victims' experiences are connected to their needs [86]. Feelings of loneliness and isolation lead to increased cybercrime victimisation [17]. Pet scams targeting pet owners have increased, with fraudsters requesting money, falsely claiming to have found a lost pet [89].

Crimes against the elderly increased during the COVID-19 pandemic [43], especially economic scams [113][36]. Correia [36] discovered that the average repeat victim was older than an average single case victim. Age also played a significant role with respect to romance fraud during the pandemic [17]. Seniors who fall victim are treated much less fairly in the UK and require special assistance to participate fully in criminal proceedings [14].

Psychological perspective: In terms of personality type, people high on neuroticism, low on conscientiousness and high on openness (to experience) are likelier to be victimised by cybercrimes [133]. Jones et al. [76] found that people who were able to proceed with cognitive reflection (i.e., suppressing incorrect information vs correct information) were moderately less prone to opening fraudulent emails. Moreover, people who scored high on sensation seeking (i.e., the personality trait of pursuing varied, novel, intense and complex experiences) were more inclined to give into automatic processes and to open fraudulent emails. Monteith et al. [102] found that even previously mentally unaffected individuals could slide into mental illness because of falling victim to cybercrime. People with pre-existing mental health conditions are particularly vulnerable to economic cybercrime. It is likely that people with a mental health conditions will experience additional obstacles to reporting if, for instance, they suffer from paranoid delusions, which can make them question their authentic experiences.

Modelling cybercrime victims: To compile an accurate victim profile, the Routine Activity Theory (RAT) is helpful [104]. The theory can be summarised as follows: people who behave insecurely online are more likely to be victimised. Nasi et al. [104] surveyed 999 respondents from the UK and matched their data with the assumptions from RAT. They found that being male, young, migrant, urban, not living with parents and unemployed with more social life online vs offline were all predictors of victimisation. Even so, caution should be exercised when discussing victim profiles so that the rhetoric does not slide into victim-blaming.

Private institution victim profiles

Bana and Hertzberg [6] found that, between 2012 and 2014, the UK's top law firms' prioritisation of cybersecurity doubled from 23 to 46 per cent. This means that nearly half of UK law firms had come to view cybersecurity as a priority, up from just under one-quarter two years earlier. This increase may have been influenced by an attack on ACS:Law, a prominent UK law firm, in 2010 [6]. Subsequent research has discussed the unexpected dip in the number of victims from private institutions despite the increased number of attacks, because of improved cybersecurity [26]. Connolly et al. [34] have found that private institutions suffer much greater harm than public institutions when attacked (p=0.044). This is because the former facing greater redundancies but also because public institutions can invest more in securing their systems. Donegan [49] argues that cybercriminals profile SMEs because these have more vulnerabilities. First, they often communicate payment correspondence via email. Second, their use of systems such as Office365 is another source of vulnerability. Third, SMEs often have publicly available information on the web that includes information about staff, which allows hackers to target those with access to funds using social engineering techniques. Connolly and Borrion [33] examine the trade-offs in victims' decision-making processes when deciding whether to pay off a ransomware attacker. Private institutions pay when they have ineffective backup, when the data are critical to the business, when there is a real risk of bankruptcy or when they follow the advice of an IT consultant.

Public institution victim profile

The WannaCry attack of 2017 cost the NHS over £93 million. In addition, Johnson [71] reports on extensive attacks aimed at the public sector in the UK, claiming that the number of ransomware attacks between 2020 and 2021 more than doubled. In 2022, the pattern of attacks mentioned by Johnson impacted UK citizens' ability to access health and social care, council tax and the like. In the case of Hackney Council, the effects of an attack cost £10 million and endangered human lives. However, the cybercrime landscape with respect to public institutions in the UK is nuanced. Take, for example, an attack on Advance in August 2022 by Ransomware [134][100]. Advance is a provider of digital services to the NHS (e.g., patient check-in) but is also a company, so is difficult to classify into one category. The attack had negative impacts on the NHS and the health of its patients.

3.3 What deters cybercrime reporting in the UK?

The first question to consider is the extent to which cybercrime victims report cybercrimes if they do fall victim. There is a great deal of evidence to show that cybercrimes are underreported [93][81]. A survey carried out in 2006 in the UK revealed that only 13 per cent of victims of cybercrime incidents had reported them [141]. To address this, some countries have created specific cybercrime reporting portals – for example Nigeria [67], Taiwan [81], the UK [2] and India [78]. These efforts attempt to address the fact that people do not always know *where* to report cybercrimes [20][10].

Despite these efforts, cybercrime continues to be underreported. It is likely that the barriers to reporting are more complex and nuanced than a technical solution could address merely by coming into being. Consider that victims may well report these kinds of crimes to their banks [81] or to their Internet service provider [141]. They may feel that these entities are better placed to help them than some country-wide reporting service.

In contemplating cybercrime reporting, we can learn from more general crime reporting, which depends on the nature of the victimisation, trust in the police, expectation that reporting will be responded to and the convenience of reporting [77][144]. It may be that a minor virus infection, which is easily ameliorated, is considered too small to merit reporting.

Some studies have specifically looked at cybercrime reporting. For example, van de Weijer et al. [136] found that Netherlands citizens would often not report cybercrime because they did not believe the police could do anything about what had happened (echoing [77][144]). McMurdie [98] suggests that people do not see any benefit in reporting cybercrimes, with Correia [37] confirming that people's perceptions of the effectiveness of police responses either deter or encourage reporting. Chawki [27] says that cybercrime victims can lose more from reporting crimes than they have already lost from the crimes themselves. Even such a perception would deter reporting. Wall [138] suggests that cybercrime may seem less significant than a violent crime such as mugging, because it is informational. People may not consider it worth reporting, perhaps because they do not realise the future implications of the information loss.

Other researchers surmise that people will not report because of a fear of being ridiculed [69]. Chawki [27] highlights reporting barriers including embarrassment, legal fees and increased insurance premiums, citing Parker [110][109]. This would align with the country's cyber-responsibilisation strategy, with citizens feeling they cannot complain since they did not follow the advice the government provided [118][119].

Reporting, or the lack thereof, is dependent on individual factors too. Gutierrez and Kirk [56] find that immigrants are less likely to report all kinds of crimes, and this is likely to apply to cybercrimes too. Holt et al. [60] find that those with less technological expertise underreport virus infections. Sometimes, cultural aspects prevent reporting, such as the need to save face [28].

Cross [40] argues that there is limited research documenting all the reasons for victims reporting, or not reporting, cybercrimes. With a relatively poorly understood range of deterrents or incentives, law enforcement does not get the reports, and cannot gain insights into the full extent of the country's cybercrime. This means it is less able to compile robust statistics [72].

In examining cybercrime reporting rigorously, several dimensions are pertinent: what kinds of cybercrimes people would report and what kinds they would simply accept; to whom they would report the crimes; and what they want from the entity they would report to. We consider the research for each of these dimensions here.

1. **Kinds of cybercrimes:** Crime type and seriousness are the largest predictors of reporting behaviour for other kinds of crimes [8][132][136]. Because cybercrime is underreported, it is difficult to answer this question definitively. What we do know is

that females are significantly more likely to report advance-fee fraud, with this effect being more pronounced in seniors [35][36]. This fraud requires victims to transfer a small amount of money with the promise of a significant return on their investment.

2. **Whom to report to:** Using a hypothetical and simulated setup, scientists presented 595 participants with vignettes about cybercrime to explore whom they would report such crimes to. People were more likely to report the offence to an organisation as opposed to the police. The exception is identity theft, which people were equally likely to report to the police and to organisations [136]. A study in Saudi Arabia [4] found that, of 267 victims, 31 per cent would not know whom to report to but would ask their friends, 15 per cent would use the Saudi government e-portal and only 7 per cent would report directly to the police.
3. **What victims want:** Victims of cyber-fraud have pronounced emotional needs, which revolve around receiving recognition from society and the police for their ordeal, which is linked to being able to tell their story [86]. Leukfeldt et al. [86] found that cybercrime victims needed to receive regular updates regarding the investigative process. Prislan et al. [115] asked people what they wanted to see post-reporting. The vast majority experienced cybercrime as a form of psychological aggression (e.g., stalking). Most people expected to see positive results if they reported to a friend in hope of getting advice (77.9 per cent) followed by the police (76 per cent).

Taxonomy of cybercrime reporting mechanisms

Baror et al. [7] suggest low levels of cybercrime reporting could be caused by a lack of clear criteria that victims can follow when reporting a crime. In fact, cybercrimes can be reported in one of three ways. We present a taxonomy of crime reporting mechanisms developed via inductive thematic analysis derived from the work of Robinson [120]. This taxonomy considers three different mechanisms for reporting: human-to-human (H2H), human-to-machine (H2M) and machine-to-machine (M2M). It should be noted that these individual categories are not independent because we cannot exclude the human element from any reporting mechanism. As such, human discretion is present in all categories, albeit to varying degrees.

H2H cybercrime reporting: H2H poses novel demands on the reporting infrastructure, which is accustomed to accepting complaints about traditional crime. Bidgoli et al. [9] present excerpts from 10 interviews of how some of their participants reported economic cybercrime using the H2H approach. One victim reported online shopping fraud to their bank to cancel their card but also to the clothing retailer Abercrombie & Fitch because the fraudulent website was mimicking the designer brand. A victim from another case study reported the computer virus to Dell customer service.

In another article, the author proposes a framework for businesses to share cybercrime knowledge [67]. The incentive for joining the voluntary initiative is the protection of the brand and service reputation. This is an example of businesses choosing to cooperate to tackle cybercrime because they realise that, while today it may be the competition that is attacked, tomorrow it could happen to them.

H2M cybercrime reporting: Heinonen et al. [58] describe reporting to the US Internet Crime Complaint Center (IC3), which receives complaints from members of the public via its online interface, but also from other organisations such as PayPal. The main strength of IC3 is that it provides helpful advice and tips on how people should protect themselves online. The main weakness is that IC3's work is insufficiently publicised to citizens.

Bidgoli et al. [10] streamlined a procedure for reporting cybercrime in PayPal. They produced a user-friendly reporting interface achieving two important goals: (1) it effectively connected reports within PayPal and outside PayPal with the relevant entities and (2) it raised awareness of cybercrime. The authors suggest that their pilot project be used by the industry and law enforcement authorities alike, even though it had not been adopted at the time of publication.

Mapimele and Mangoale [97] devised an H2M reporting platform called the Cybercrime Combating Platform (CP3). The CP3 algorithms allow users to search for compromises of their data. The system makes use of databases to trawl through online cybercrime activities. The databases it engages with are HaveIBeenPwnd, Phishtank, Dshield and Breach Level Index.

An independent analysis of the ACORN system discovered that victims who reported to the ACORN online system experienced high levels of dissatisfaction [41]. Specifically, 77 per cent of complainants were unhappy with the outcome of their complaint. This is perhaps because the data captured by ACORN were of poor quality. Moreover, reports were stored in an unorganised text format, which made investigation problematic. This highlights the fact that cybercrime reporting should not be reduced to a mere transfer of information about an offence. Rather, everything related to the reporting interface should be designed with great care and in consultation with members of the public. In particular, the way the information is stored and subsequently analysed should be transparent to reporters [46] and helpful to law enforcement in terms of apprehending the perpetrator.

M2M cybercrime reporting: Carpineto and Romano [25] designed an automated pipeline with two machine learning stages to identify sellers of counterfeit luxurious clothes. This prototype was found to be more effective than established trustworthiness systems and non-expert humans.

Sheikhalishahi et al. [126] designed an automated analysis and classification of spam email pilot. The authors proposed an automatic method and resulting framework founded on pioneering categorical divisive clustering, which was successfully tested on a dataset retrieved from honeypots.

A technological development by Singh et al. [127] delved into identifying the difference between a phishing website and a classical web page. This task was challenging because of its semantic structure. Singh et al. managed to apply a phishing detection system by utilising deep learning mechanisms. The framework engages URLs via an application of the Convolutional Neural Network (CNN) with an accuracy of 98 per cent. The CNN is a type of deep learning algorithm capable of inputting, analysing, and differentiating between images. This system produces an outcome of its activity as a classification report where it classifies URLs as either 'phishing' or 'legitimate'. Currently, this system is just a prototype awaiting deployment in the wider cybersecurity stratosphere.

Policing cybercrime

The way cybercrime is policed, and perceptions related to such policing, is inextricably linked to cybercrime reporting. Hence it is worth discussing these aspects when we are considering cybercrime reporting. Policing of cybercrime has several dimensions, which we discuss now.

Connection between traditional and cybercrime: Cybercrime researchers debate the policing of cybercrime. Some attempt to adapt the principles from traditional crime policing onto cybercrime [64][65]. Others highlight the insufficiency of the cybercrime-related training of police forces [52][92][122]. This can be the result of a vicious circle whereby the police do not feel the same enthusiasm for pursuing cybercrime vs traditional crime, with which they are more familiar. This feeds into poor training standards and uptake. As a result, police are sometimes not equipped with the skills required to solve cybercrimes, which compromises their ability to pursue cybercriminals. Constables who engage in cybercrime training do indeed feel they are more prepared to deal with reported cybercrimes [12]. It has been found that face-to-face training is more effective than online training [30]. In addition, police forces would benefit from clear guidelines for cybercrime policing [12]. This is challenging because the English system is highly decentralised, which would create disagreement [72]. A human resources piece explored the new role of Digital Media Investigators (DMIs) in the UK [141]. The DMIs were created by up-skilling police officers to use technology to relieve the specialised teams from mundane tasks.

Challenges: Yadav et al. [147] reported on a case study of actual reporting related to an offender who had created abusive websites to target various actors in the art business and who had managed to extort over $3 million from his victims. The offender used multiple fake accounts, each of which had to be individually reported and linked to identify the single attacker.

Cross [42] talks about the problems of jurisdiction that police face, such as cases when the offender commits the crime from abroad against a home national. This makes it difficult to determine in which jurisdiction the crime took place.

Meanwhile, victims who report cybercrimes often have misconceptions about the various policing bodies in Australia. Cross [42] argues for greater transparency as well as more awareness-raising about the competencies and limitations of investigations.

Hadlington et al. [57] reported on interviews with 16 frontline police officers to examine the crucial aspects of cybercrime. The police staff said they continued to struggle with how to define cybercrime, with its constantly evolving nature and with the lack of appropriate training that would help them remain on the cutting edge. This is simply a new type of situation to which humanity needs time to adapt.

Models: Hunton [64] has developed a model for cybercrime policing. In Stage 1, the investigation of the offence starts. During Stage 2, the cybercrime is modelled. During Stage 3, a specialist assessment of what is known takes place. The purpose of Stage 4 is risk assessment. Investigation planning takes place as a part of Stage 5. The activities in Stage 6 are focused on handling data to keep evidence intact. Stage 7 is the carrying-out of the intervention and Stage 8 presents the results.

Roles: Hunton [65] identifies five policing roles within the investigation framework, organised based on a hierarchical power principle. The main strengths of this model are its functional specialisation and division of labour. The main weakness may be its rigidity, which can get in the way of accepting ideas from staff seen as lower on the pecking order.

Organisation: The police are navigating their activity in a sector that originally fell under the private sector [138]. As an example of the increasing controversy surrounding this merger, a trend has been observed whereby the police rely on the private sector to assist with cybercrime policing [72]. The UK police have evaluated the effectiveness of local policing [48]. In 2018, it was found that the force did not have an established line of communication with the National Crime Agency to pass on information about cybercrime. This may have changed some four years later. It is also worth noting examples that highlight the analytical capabilities of the police [124]. Lastly, it is worth mentioning 'influence policing', which is based around the digital footprint of at-risk Internet users. This is used to tailor deterrence ads [32].

Human resources: Obstacles to cybercrime policing can range from inter-agency competition to lack of resources to hire specialised staff [129]. An integral part of human resources is development. The London Met have rolled out the Ncalt training package, which is an online cybercrime training that has drawn some criticism as most police officers from the study felt under-trained [45]. Problems with training are a theme that re-emerges in research [53][122]. As a solution to this issue, a local police force boosted its expertise by hiring a former hacker [92]. Since 2003, the problem of cyber-fraud is also policed by vigilantes [21].

Jurisprudence: Current laws can challenge the policing of cybercrime [95]. Examples of challenges include using a fake social media profile to access information on social media, which is an offence under the Computer Misuse Act 1990. Moreover, specific national differences in legal definitions affect investigations and prosecutions. For example, not every group of organised criminals constitutes organised crime [85].

It has been argued that current legal approaches focus on conceptualising the systems of crime but fall behind offenders. What might be required is a bespoke force of dedicated online constables [121]. Lastly, Brexit has affected cybercrime jurisprudence. According to Stevens and O'Brein [131], Brexit affects the UK's capabilities in terms of policing and sentencing cybercrime by loosening ties with Europol and the European courts.

Community policing: It has been suggested that the links between the local police and communities could provide a network that can work to improve cybercrime reporting in a democratic way. Horgan et al. [62] suggest harnessing the power of community links with the police. It can only be added that the insider's view of the community police may be useful in filling many of the holes that are contained within cybercrime reports. This argument is in line with the favourable view that Wooff et al. [145][146] have towards community policing.

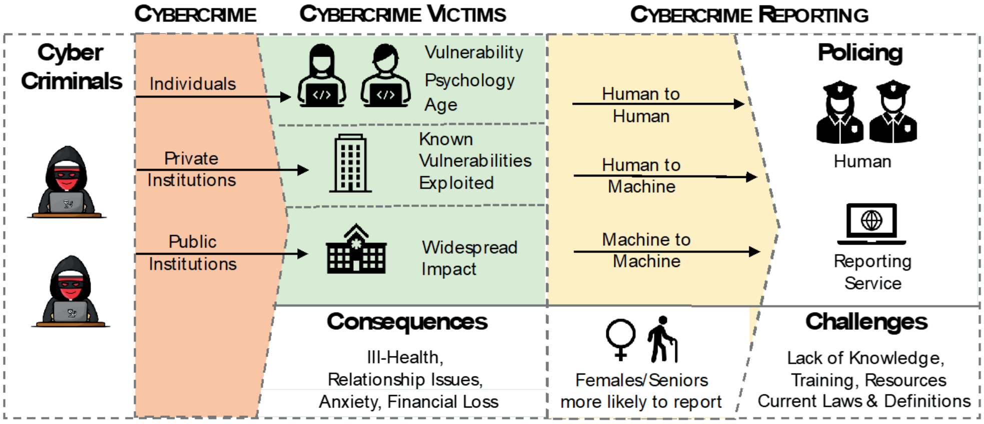
Choi and Lee [29] find that, in the UK, citizens are willing to participate in voluntary policing in their communities because it gives them a sense of authority, respect and recognition as well as a potential trajectory into a policing career. Hence, broader engagement with community resources could mobilise citizens to help their vulnerable neighbours stay safe from and report economic cybercrime.

Cybercrime reporting: final comments

In Australia, Cross [38] found that people's reporting experiences were often influenced by overestimation of the police force's capabilities. She coined this the 'CSI effect', based on the popular TV crime show. This means that people's expectations of the police are unrealistically high based on what they see on TV. On CSI, all investigations run smoothly and successfully. Consequently, victims are disappointed if their cases do not meet their expectations.

Figure 2 summarises this section. The next section addresses each of the research questions in turn.

Figure 2: Summary of the discussion in this section



4. Discussion

We now return to the original research questions.

RQ1: What characterises cybercrime in the UK?

The UK is clearly a target for cybercriminals, because of the high percentage of retail sales that occurs online in the UK (24.8 per cent [109]). This constitutes a massive opportunity for criminals, with the UK being in the top 10 countries targeted by cybercriminals. In 2021, the UK lost £1.3 billion to cybercrime and fraud [124], so there is a considerable need to maximise cybercrime reporting to ensure cybercriminals are apprehended and prosecuted.

RQ2: What is known about UK cybercrime victims?

It has been reported that one in five UK citizens has been a victim of cybercrime [54]. The same report found that Wales was the worst region for cybercrime, with Scotland least affected. However, these figures are based on data from Action Fraud and, since cybercrimes are underreported, the true figures could be much higher.

RQ3: What influences and deters cybercrime reporting in the UK?

Responsibilisation is a strategy applied by the UK government, which provides a great deal of advice on how to prevent cybercrime and expects citizens to follow this. In the UK, this strategy may well be contributing to underreporting of cybercrimes in three ways.

1. The responsibilisation agenda assigns responsibility to citizens to take care of their own cybersecurity. If people fall victim to an attack, they are like to blame themselves for it. Reporting the crime may be perceived as an admission of their own failure. This may discourage reporting.

2. Raising awareness of the need for cybercrime reporting, and disseminating ways of doing this, is not receiving the investment it should, leaving citizens confused.
3. The 'Cybercrime Reporting' section of the UK's Victim Support website [137] says: 'Please note that it's no longer possible to report fraud to your local police station – Action Fraud is the national fraud reporting service and is the starting point for any police investigation into your loss.' This is bound to be confusing, given that all other crimes are reported to the police.

Technological solutions are insufficient. If reporting were dependent merely on a technical system being available to collect reports, underreporting should not persist, since such systems exist in the UK. It has become clear, then, that merely making such systems available does not, in and of itself, encourage reporting. Bossler [12] argues that cybercrime reporting could be improved with a set of 'best practice' procedures and guidelines rolled out across the board. This idea has been questioned by Johnson et al. [72] because the decentralisation of the English force makes this infeasible. In contrast, the centralised Scottish force may be able to test this idea [103]. Even so, merely having such a set of processes and procedures does not guarantee that citizens will engage in them.

Responses to reports must be seen as effective. If people report an attack and do not believe the police have taken their cybercrime report seriously or attempted to apprehend the criminal, they may well not report further cybercrimes.

An oft-neglected dimension to reporting is related to societal norms and context. Such societal aspects are likely to play an important role in the compilation of accurate reports. Previous research has also supplied inferential evidence to suggest that cybercrime reporting should be treated as a social interaction [80], which could improve reporting by vulnerable populations [98].

People may well believe they deserve to lose money because they have not followed the provided advice. They may also keep quiet if they think their peers would think less of them if they have fallen for a con.

We must consider all these influences if we want to encourage cybercrime reporting – and not only the availability, accessibility and usability of the technical systems that people can use to report cybercrimes.

Research implications

There is a clear need to develop reporting systems that people will be more likely to use. It would be helpful to model cybercrime reporting, and its deterrents, to better understand the factors that encourage and/or discourage cybercrime reporting. Once the influential factors have been identified, the next step would be to identify interventions to mitigate the deterring factors and to enhance those factors that motivate victims to report cybercrimes.

5. Conclusion

A systematic literature review was conducted to explore questions around UK cybercrime, to answer the questions: What characterises cybercrime in the UK? What is known about UK cybercrime victims? and What influences and deters cybercrime reporting in the UK?

We discovered that UK is experiencing increasing levels of cybercrime, which has been exacerbated by the pandemic lockdowns. UK citizens tend to shop more online than do citizens of other countries, meaning that the potential to fall victim to cybercrimes is high. However, the full extent of UK citizen victimisation is not well understood, owing to cybercrime underreporting. The UK's responsibilisation agenda may be contributing to low levels of cybercrime reporting: reporting is likely to remain low if victims blame themselves for their victimisation. To improve reporting prevalence, we must focus on all dimensions of underreporting systems, all the way from technical to societal deterrents.

References

[1] Abdulai, M.A. (2020) 'Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud'. *International Journal of Cyber Criminology* 14(1): 157–174. https://doi.org/10.5281/zenodo.3749468

[2] Action Fraud (nd) '24 Hour Live Cyber Reporting for Businesses'. www.actionfraud.police.uk/

[3] Akdemir, N. and Lawless, C.J. (2020) 'Exploring the Human Factor in Cyber-enabled and Cyberdependent Crime Victimisation: A Lifestyle Routine Activities Approach'. *Human Factor in Cybercrime Victimisation* 30(6): 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

[4] Alzubaidi, A. (2021) 'Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia'. *Heliyon* 7(1): e06016.

[5] Arora, B. (2016) 'Exploring and Analyzing Internet Crimes and Their Behaviours'. *Perspectives in Science* 8: 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

[6] Bana, A. and Hertzberg, D. (2015) 'Data Security and the Legal Profession: Risks, Unique Challenges and Practical Considerations'. *Business International Law* 16(3): 247–264.

[7] Baror, S.O., Ikuesan, R.A. and Venter, H.S. (2020) 'A Defined Digital Forensic Criteria for Cybercrime Reporting'. Proceedings of the 15th International Conference on Cyber Warfare and Security: 617–626.

[8] Bennett, R.R. and Wiegand, R.B. (1994) 'Observations on Crime Reporting in a Developing-Nation'. *Criminology* 32(1): 135–148. https://doi.org/10.1111/j.1745-9125.1994.tb01149.x

[9] Bidgoli, M., Knijnenburg, B.P. and Grossklags, J. (2016) 'When Cybercrimes Strike Undergraduates'. *eCrime Researchers Summit, eCrime*: 42–51. https://doi.org/10.1109/ECRIME.2016.7487948

[10] Bidgoli, M., Knijnenburg, B.P., Grossklags, J. and Wardman, B. (2019) 'Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting'. *eCrime Researchers Summit, eCrime*: 1–10. https://doi.org/10.1109/eCrime47957.2019.9037577

[11] Böhme, R. (2013) *The Economics of Information Security and Privacy*. Heidelberg, New York, Dordrecht, London: Springer.

[12] Bossler, A.M., Holt, T.J., Cross, C. and Burruss, G.W. (2020) 'Policing Fraud in England and

Wales: Examining Constables' and Sergeants' Online Fraud Preparedness'. *Security Journal* 33: 311–328. https://doi.org/10.1057/s41284-019-00187-5

[13] Boyce, C.J. and Wood, A.M. (2010) 'Money or Mental Health: The Cost of Alleviating Psychological Distress with Monetary Compensation Versus Psychological Therapy'. *Health Economics, Policy and Law* 5(4): 509–516. https://doi.org/10.1017/S1744133109990326

[14] Bowles, R., Garcia Reyes, M. and Garoupa, N. (2009) 'Crime Reporting Decisions and the Costs of Crime'. *European Journal on Criminal Policy and Research* 15(4): 365–377. https://doi.org/10.1007/s10610-009-9109-8

[15] Brenner, S.W. (2007) 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare'. *Journal of Criminal Law and Criminology* 97(2): 379–476. https://www.jstor.org/stable/40042831

[16] Brown, K.J. and Gordon, F. (2022) 'Improving Access to Justice for Older Victims of Crime by Reimagining Conceptions of Vulnerability'. *Ageing and Society* 42(3): 614–631. https://doi.org/10.1017/S0144686X20001051

[17] Buil-Gil, D. and Saldana-Taboada, P. (2021) 'Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime'. *Deviant Behavior* 43(12): 1–18. https://doi.org/10.1080/01639625.2021.1988760

[18] Buil-Gil, D. & Zeng, Y. (2021) 'Meeting You Was a Fake: Investigating the Increase in Romance Fraud during COVID-19'. *Journal of Financial Crime* 29(2): 460–475. https://doi.org/10.1108/JFC-02-2021-0042

[19] Buil-Gil, D., Miro-Llinares, F., Moneva, A. et al. (2021) 'Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK'. *European Societies* 23(S1): S47–S49. https://doi.org/10.1080/14616696.2020.1804973

[20] Burgard, A. and Schlembach, C. (2013) 'Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet'. *International Journal of Cyber Criminology* 7(2): 112.

[21] Button, M. and Whittaker, J. (2021) 'Exploring the Voluntary Response to Cyber-Fraud: From vigilantism to responsibilisation'. *International Journal of Law, Crime and Justice* 66: 100482. https://doi.org/10.1016/j.ijlcj.2021.100482

[22] Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. (2014) 'Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408. https://doi.org/10.1177/0004865814521224

[23] Böhme, R. and Moore, T. (2012) 'How Do Consumers React to Cybercrime?' eCrime Researchers Summit, Las Croabas, Puerto Rico, 22–25 October. https://doi.org/10.1109/eCrime.2012.6489519

[24] Caneppele, S. and 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. https://doi.org/10.1093/police/pax055

[25] Carpineto, C. and Romano, G. (2020) 'An Experimental Study of Automatic Detection and Measurement of Counterfeit in Brand Search Results'. *ACM Transactions on the Web* 14(2): 1–35. https://doi.org/10.1145/3378443

[26] CFS (2018) 'Number of Cybercrime Victims Falls'. *Computer Fraud & Security* 5: 20. https://doi.org/10.1016/S1361-3723(18)30045-9

[27] Chawki, M. (2005) 'A Critical Look at the Regulation of Cybercrime'. *The ICFAI Journal of Cyberlaw* IV(4).

[28] Cheng, C., Chau, M.C.L. and Chan, M.L. (2018) 'A Social Psychological Analysis of the Phenomenon of Underreporting Cybercrimes and the Concomitant Underlying Factors: Three Real Local Case Studies'. *Communications Association of Hong Kong*.

[29] Choi, K. and Lee, J. (2016) 'Citizen Participation in Community Safety: A Comparative Study of Community Policing in South Korea and the UK'. *Policing & Society* 26(2): 165–184. https://doi.org/10.1080/10439463.2014.922087

[30] Cockroft, T., Shan-A-Khuda, M., Schreuders, Z.C. and Trevorrow, P. (2021) 'Police Cybercrime Training: Perceptions, Pedagogy, and Policy'. *Policing: A Journal of Policy and Practice* 15(1): 15–33. https://doi.org/10.1093/police/pay078

[31] Collier, D., Thomas, D.R., Clayton, R. and Hutchings, A. (2019) 'Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks'. Proceedings of the Internet Measurement Conference, October. https://doi.org/10.1145/3355369.3355592

[32] Collier, D., Thomas, D.R., Clayton, R. et al. (2021) 'Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market of Cybercrime Services'. *Policing & Society. An International Journal of Research and Policy* 32(1): 103–124. https://doi.org/10.1080/10439463.2021.1883608

[33] Connolly, A.Y. and Borrison, H. (2020) 'Your Money or Your Business'. Proceedings of the 41st International Conference on Information Systems. Association for Information Systems. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/6

[34] Connolly, A.Y., Wall, D.S., Lang, M. and Oddson, B. (2020) 'An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability'. *Journal of Cybersecurity* 6(1): tyaa023. https://doi.org/10.1093/cybsec/tyaa023

[35] Correia, S.G. (2019) 'Responding to Victimisation in a Digital World: A Case Study of Fraud and Computer Misuse Reported in Wales'. *Crime Science* 8(4): 1–12. https://doi.org/10.1186/s40163-019-0099-7

[36] Correia, S.G. (2020) 'Patterns of Online Repeat Victimisation and Implications for Crime Prevention'. 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA. https://doi.org/10.1109/eCrime51433.2020.9493258

[37] Correia, S.G. (2022) 'Making the Most of Cybercrime and Fraud Crime Report Data: A Case Study of UK Action Fraud'. *International Journal of Population Data Science* 7(1): 9. https://doi.org/10.23889/ijpds.v7i1.1721

[38] Cross, C. (2018) 'Expectations vs. Reality: Responding to Online Fraud across the Fraud Justice Network'. *International Journal of Law, Crime and Justice* 55: 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

[39] Cross, C. (2019) 'Is Online Fraud Just Fraud? Examining the Efficacy of the Digital Divide'. *Journal of Criminological Research, Policy and Practice* 5(2): 120–131. https://doi.org/10.1108/JCRPP-01-2019-0008

[40] Cross, C. (2019) 'Responding to Individual Fraud'. In E.R. Leukfeldt and T.J. Holt (eds) *The Human Factor of Cybercrime* (pp. 359–388). Abingdon: Routledge.

[41] Cross, C. (2020) 'Reflections on the Reporting of Fraud in Australia'. *Policing* 43(1): 49–61. https://doi.org/10.1108/PIJPSM-08-2019-0134

[42] Cross, C. (2020) '"Oh We Can't Actually Do Anything about That": The Problematic Nature of Jurisdiction for Online Fraud Victims'. *Criminology and Criminal Justice* 20(3): 358–375.

[43] Cross, C. (2021) 'Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons'. *The Journal of Adult Protection* 23(2): 98–109. https://doi.org/10.1108/JAP-08-2020-0035

[44] Cross, C. and Kelly, M. (2016) 'The Problem of "White Noise": Examining Current Prevention Approaches to Online Fraud'. *Journal of Financial Crime* 23(4): 806–818. https://doi.org/10.1108/JFC-12-2015-0069

[45] Cross, C., Holt, T., Powell, A. and Wilson, M. (2018) 'Responding to Cybercrime: Results of a Comparison between Community Members and Police Personnel'. *Trends and Issues in Crime and Criminal Justice* 635: 1–20.

[46] Das, A., Nayak, J. Naik, B. and Ghosh, U. (2021) 'Generation of Overlapping Clusters Constructing Suitable Graph for Crime Report Analysis'. *Future Generation Computer Systems: The International Journal Of EScience* 118: 339–357. https://doi.org/10.1016/j.future.2021.01.027

[47] Department for Digital, Culture, Media & Sport (2022) 'Cyber Security Breaches Survey'. www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[48] Doig, A. (2018) 'Implementing National Policing Agendas and Strategies for Fraud at Local Level'. *Journal of Financial Crime* 25(4): 984–996. https://doi.org/10.1108/JFC-04-2017-0027

[49] Donegan, M. (2019) 'Crime Script for Mandate Fraud'. *Journal of Money Laundering* 22(4): 770–781. https://doi.org/10.1108/JMLC-03-2019-0025

[50] Elkin, M. (2022) 'Crime in England and Wales: Year Ending December 2021'. www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2021#computer-misuse

[51] Fisher, J. (2008) 'The UK's Faster Payment Project: Avoiding a Bonanza for Cybercrime Fraudsters'. *Journal of Financial Crime* 15(2): 155–164. https://doi.org/10.1108/13590790810866872

[52] Fleming, J. (2022) 'Director GCHQ Speaks at CyberUK 2022'. GCHQ speech, 10 May www.gchq.gov.uk/speech/cyberuk2022

[53] 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 H. Jahankhani (ed.) *Cyber Criminology. Advanced Sciences and Technologies for Security Applications* (pp. 307–323). Amsterdam: Springer.

[54] Fox, H. (2022) 'The Worst UK Regions for Cybercrime'. *Ocean Finance News*, 22 April. www.oceanfinance.co.uk/blog/the-worst-uk-regions-for-cybercrime/

[55] Goudriaan, H., Wittebrood, K. and Nieuwbeerta, P. (2006) 'Neighbourhood Characteristics and Reporting Crime Effects of Social Cohesion, Confidence in Police Effectiveness and Socio-Economic Disadvantage'. *British Journal of Criminology* 46(4): 719-742. https://doi.org/10.1093/bjc/azi096

[56] Gutierrez C.M. and Kirk D.S. (2017) 'Silence Speaks: The Relationship between Immigration and the Underreporting of Crime'. *Crime Delinq.* 63(8): 926–950. https://doi.org/10.1177/0011128715599993

[57] Hadlington, L., Lumsden, K. Black, A. and 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. https://doi.org/10.1093/police/pay090

[58] Heinonen, J.A., Holt, T.J. and Wilson, J.M. (2012) 'Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics'. *International Criminal Justice Review* 22(4): 353–371.

[59] HMICFRS (2020) 'A Call for Help: Police Contact Management through Call Handling and Control Rooms in 2018/19'. Technical Report.

[60] Holt, T.J., VanWilsem, J., Van deWeijer, S.G.A. and Leukfeldt, E.R. (2018) 'Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization'. *Social Science Computer Review* 38(2). https://doi.org/10.1177/0894439318805067

[61] Horgan, S. (2021) 'The Reality of "Cyber Security Awareness": Findings and Policy Implications for Scotland'. Scottish Justice Fellowship Briefing Paper.

[62] Horgan, S., Collier, B. Jones, R. and 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* 11(3): 222–239. https://doi.org/10.1108/JCP-08-2020-0034

[63] Hunter, P. (2008) 'UK Shadow Home Secretary Victim of Online Card Fraud'. *Computer Fraud & Security* 6: 4. https://doi.org/10.1016/S1361-3723(08)70094-0

[64] Hunton, P. (2011) 'A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment'. *Digital Investigation* 7(3): 105–113. https://doi.org/10.1016/j.diin.2011.01.002

[65] Hunton, P. (2012) 'Managing the Technical Resource Capability of Cybercrime Investigation: A UK Law Enforcement Perspective'. *Public Money and Management* 32(3): 225–232. https://doi.org/10.1080/09540962.2012.676281

[66] Hutchings, A. and Pastrana, S. (2019) 'Understanding eWhoring'. 4th IEEE European Symposium on Security and Privacy, Stockholm, 17–19 June. https://doi.org/10.1109/EuroSP.2019.00024

[67] Ismail, U. (2020) 'The Nigeria Police Force and Cybercrime Policing: An Appraisal'. *Dutse Journal of Criminology and Security Studies* 1: 78–88.

[68] ISACA (2019) 'State of Cybersecurity 2019 Part 2: Current Trends in Attacks, Awareness and Governance'. Press Release, November.

[69] Jaishankar, K. (2020) 'Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology'. In J. Joseph (ed.) *An International Perspective on Contemporary Developments in Victimology* (pp. 3-19). Heidelberg, New York, Dordrecht, London: Springer.

[70] Jhaveri, M.H. Cetin, O. Gañán, C. et al. (2017) 'Abuse Reporting and the Fight against Cybercrime'. *Comput. Surveys* 49(4): 1–27. https://doi.org/10.1145/3003147

[71] Johnson, B. (2022) 'Improving the State of Cyber Security in the Public Sector'. Government Business. https://governmentbusiness.co.uk/features/improving-state-cyber-security-public-sector

[72] Johnson, D., Faulkner, E., Meredith, G. and Wilson, T.J. (2020) 'Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts'. *Journal of Criminal Law* 84(5): 427–450.

[73] Johnson, J. (2021) 'Cyber Crime and UK Consumers: Statistics & Facts'. www.statista.com/topics/8416/cyber-crime-and-ukconsumers/

[74] Johnson, J. (2021) 'Cyber Crime and UK Consumers – Statistics & Facts'. Statista. https://www.statista.com/topics/8416/cyber-crime-and-uk-consumers/

[75] Jones, C. (2022) 'Ransomware Strikes Scottish Mental Health Charity. *ITPro*, 21 March. www.itpro.co.uk/security/ransomware/367137/scottish-association-mental-health-ransomware

[76] Jones, H.S., Towse, J.N., Race, N. and Harrison, T. (2019) 'Email Fraud: The Search for Psychological Predictors of Susceptibility'. *Plos One* 14(1): e0209684. https://doi.org/10.1371/journal.pone.0209684

[77] Junger-Tas, J. and Marshall, I.H. (1999) 'The Self-Report Methodology in Crime Research'. *Crime and Justice* 25: 291-367. https://doi.org/10.1086/449291

[78] Kaur, M. and Saini, M. (2022) 'Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions'. *Education and Information Technologies* 46(3): 1–35. https://doi.org/10.1007/s10639-022-11168-4

[79] Kemp, S. Buil-Gil, D., Moneva, A. et al. (2021) 'Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends during COVID-19'. *Journal Of Contemporary Criminal Justice* 37(4): 480–501. https://doi.org/10.1177/10439862211027986

[80] Kieckhaefer, J.M., Vallano, J.P. and Compo, N.S. (2014) 'Examining the Positive Effects of Rapport Building: When and Why Does Rapport Building Benefit Adult Eyewitness Memory?' *Memory* 22(8): 1010–1023. https://doi.org/10.1080/09658211.2013.864313

[81] Kuo, T.L. (2022) 'Criminal Victimisation in Taiwan: An Opportunity Perspective'. Doctoral dissertation, University College London.

[82] Langton, L., Berzofsky, M., Krebs, C. and Smiley-McDonald, H. (2012) 'Victimizations Not Reported to the Police, 2006-2010'. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

[83] Lavorgna, A. (2019) 'Cyber-Organised Crime. A Case of Moral Panic?' *Trends in Organized Crime* 22: 357–374. https://doi.org/10.1007/s12117-018-9342-y

[84] Leukfeldt, E.R. Kleemans, E.R. and Stol, W.P. (2017) 'Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis'. *Crime, Law and Social Change* 67: 39–53. https://doi.org/10.1007/s10611-016-9663-1

[85] Leukfeldt, E.R., Lavorgna, A. and Kleemans, E.R. (2017) 'Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime'. *European Journal on Criminal Policy and Research* 23(33): 287–300. https://doi.org/10.1007/s10610-016-9332-z

[86] Leukfeldt, E.R., Notte, R.J. and Malsch, M. (2020) 'Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes'. *Victims & Offenders* 15(1): 60–77. https://doi.org/10.1080/15564886.2019.1672229

[87] Levi, M. (2017) 'Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues'. *Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change. Crime, Law and Social Change* 67: 3–20. https://doi.org/10.1007/s10611-016-9645-3

[88] Levi, M., Doig, A. Gundur, R. Wall, D. and Williams, M. (2017) 'Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research'. *Crime, Law and Social Change* 67(1): 77–96. https://doi.org/10.1007/s10611-016-9648-0

[89] Levi, M. and Smith, R.G. (2021) 'Fraud and Pandemics'. *Journal of Financial Crime* 29(2): 413–432. https://doi.org/10.1108/JFC-06-2021-0137

[90] Levi, M. and Williams, M.L. (2013) 'Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space'. *Information Management & Computer Security* 21(5): 420–443. https://doi.org/10.1108/IMCS-04-2013-0027

[91] Lord, J. (2016) 'Fifty Shades of Fraud'. *Computer Fraud & Security* 6: 14–16. https://doi.org/10.1016/S1361-3723(15)30047-6

[92] Loveday, B. (2018) 'The Shape of Things to Come. Reflections on the Potential Implications of the 2016 Office of National Statistics Crime Survey for the Police Service of England and Wales'. *Policing: A Journal of Policy and Practice* 12(4): 398–409. https://doi.org/10.1093/police/pax040

[93] Lovet, G. (2009) 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges'. Virus Bulletin Conference, September. www.virusbulletin.com/conference/vb2009/abstracts/fighting-cybercrime-technical-juridical-and-ethical-challenges/

[94] Lufkin, B. (2020) 'The Curious Origins of Online Shopping'. BBC, 27 July. www.bbc.com/worklife/article/20200722-the-curious-origins-of-online-shopping

[95] Lyle, A. (2016) 'Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism'. In *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications* (pp. 277–294). Amsterdam: Springer.

[96] Maltz, M.D. (1977) 'Crime Statistics: A Historical Perspective'. *Crime & Delinquency* 23(1): 32–40.

[97] Mapimele, F. and Mangoale, B. (2019) 'The Cybercrime Combating Platform'. In N. van der Waag-Cowling and L. Leenen (eds) *14th International Conference on Cyber Warfare and Security* (pp. 237–242). Stellenbosch.

[98] McMurdie, C. (2016) 'The Cybercrime Landscape and Our Policing Response'. *Journal of Cyber Policy* 1(1): 85–93. https://doi.org/10.1080/23738871.2016.1168607

[99] Middle East Post Box (nd) '10 Countries Whose Residents Are Most Enticing For Cybercriminals'. https://middleeastpostbox.com/10-countries-whose-residents-are-most-enticing-for-cybercriminals/

[100] Milmo, D. (2022) 'NHS Ransomware Attack: What Happened and How Bad Is It?' *The Guardian*, 11 August. www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

[101] Milne, R. and Bull, R. (2001) 'Interviewing Witnesses with Learning Disabilities for Legal Purposes'. *British Journal of Learning Disabilities* 29: 93–97. https://doi.org/10.1046/j.1468-3156.2001.00139.x

[102] Monteith, S., Bauer, M., Alda, M. et al. (2021) 'Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry'. *Current Psychiatry Reports* 23(4): 1–9. https://doi.org/10.1007/s11920-021-01228-w

[103] Murray, K. and Harkin, D. (2017) 'Policing in Cool and Hot Climates: Legitimacy, Power and the Rise and Fall of Mass Stop and Search in Scotland'. *British Journal of Criminology* 57(4): 885–905. https://doi.org/10.1093/bjc/azw007

[104] Nasi, M., Oksanen, A., Keipi, T. and Rasanen, P. (2015) 'Cybercrime Victimization among Young People: A Multi-Nation Study'. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16(2): 203–210. https://doi.org/10.1080/14043858.2015.1046640

[105] NCA (2020) *National Strategic Assessment of Serious and Organised Crime*. London: NCA. www.nationalcrimeagency.gov.uk/news/nsa2020

[106] NHS (nd) 'Prevention Is the Best Defence'. https://nhsfraudandsecurity.co.uk/security-information/cyber-crime

[107] ONS (2021) 'Crime in England and Wales QMI'. www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/crimeinenglandandwalesqmi

[108] ONS (2021) 'Crime in England and Wales, Year Ending December 2020—Appendix Tables'. www.ons.gov.uk/releases/crimeinenglandandwalesyearendingdec2020

[109] ONS (2021, February 17) 'Internet Sales as a Percentage of Total Retail Sales'. www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi

[110] Parker, D.B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, Inc.

[111] Pastrana, S. Hutchings, A., Thomas, D.R. and Tapiador, J. (2019) 'Measuring eWhoring'. Proceedings of the Internet Measurement Conference: 463–477.

[112] Pickering, C., Grignon, J., Steven, R. et al. (2015) 'Publishing Not Perishing: How Research Students Transition from Novice to Knowledgeable Using Systematic Quantitative Literature Reviews'. *Studies in Higher Education* 40(10): 1756–1769. https://doi.org/10.1080/03075079.2014.914907

[113] Police Scotland and Scottish Police Authority (2020) *Cyber Strategy 2020: Keeping People Safe in the Digital World*. www.scotland.police.uk/spa-media/vz0d3v31/cyber-strategy.pdf

[114] Popham, J., McCluskey, M., Ouellet, M. and Gallupe, O. (2020) 'Exploring P-reported Cybercrime in Canada: Variation and Correlates'. *Policing* 43(1): 35–48. https://doi.org/10.1108/PIJPSM-08-2019-0128

[115] Prislan, K., Bernik, I., Mesko, G. et al. (2019) 'Cybercrime Victimization and Seeking Help: A Survey of Students in Slovenia'. *Third Central European Cybersecurity Conference* 1–2. https://doi.org/10.1145/3360664.3360731

[116] Protrka, N. (2021) 'Cybercrime', in M. Roycroft and L. Brine (eds) *Modern Police Leadership* (pp. 143-155). Basingstoke: Palgrave Macmillan.

[117] Reep-van den Bergh, C.M.M. and Junger, M. (2018) 'Victims of Cybercrime in Europe: A Review of Victim Surveys'. *Crime Science* 7(1): 1–15. https://doi.org/10.1186/s40163-018-0079-3

[118] Renaud, K., Flowerday, S., Warkentin, M. et al. (2018) 'Is the Responsibilisation of the Cyber Security Risk Reasonable and Judicious?' *Computers & Security* 78: 198–211. https://doi.org/10.1016/j.cose.2018.06.006

[119] Renaud, K., Orgeron, C., Warkentin, M. and French, P.E. (2020) 'Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China'. *Public Administration Review* 80(4): 577–589. https://doi.org/10.1111/puar.13210

[120] Robinson, O.C. (2022) 'Conducting Thematic Analysis on Brief Texts: The Structured Tabular Approach'. *Qualitative Psychology* 9(2): 194–208. https://doi.org/10.1037/qup0000189

[121] Sampson, F. (2014) 'Cyberspace: The New Frontier for Policing?' In B. Akhgar, A. Staniforth and F. Bosco (eds) *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 1–10). Amsterdam: Syngress.

[122] Schreuders, Z.C., Cockroft, T., Elliott, J. et al. (2020) 'Needs Assessment of Cybercrime and

Digital Evidence in a UK Police Force'. *International Journal of Cyber Criminology* 14(1): 316–340. https://doi.org/10.5281/zenodo.3757271

[123] Scroxton, A. (2021) 'Fraud and Cyber Crime Still Vastly Under-Reported'. *Computer Weekly*, 4 February. www.computerweekly.com/news/252495844/Fraud-and-cyber-crime-still-vastly-under-reported

[124] Scroxton, A. (2021) 'UK Loses £1.3bn to Fraud and Cyber Crime So Far This Year'. *Computer Weekly*, 25 August. www.computerweekly.com/news/252505825/UK-loses-13bn-to-fraud-and-cyber-crime-so-far-this-year

[125] Shan-A-Khuda, M. and Schreuders, Z.C. (2019) 'Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis'. *International Journal of Cyber Criminology* 13(2): 493–510. https://doi.org/10.5281/zenodo.3708924

[126] Sheikhalishahi, M., Saracino, A., Martinelli, F. et al. (2020) 'Digital Waste Disposal: An Automated Framework for Analysis of Spam Emails'. *International Journal of Information Security* 19(5): 499–522. https://doi.org/10.1007/s10207-019-00470-x

[127] Singh, S., Singh, M.P. and Pandey, R. (2020) 'Phishing Detection from URLs Using Deep Learning Approach'. Proceedings of the 2020 5th International Conference on Computing, Communication and Security: 1–4.

[128] Singh, S.K. and Rastogi, N. (2018) 'Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study'. 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages. https://doi.org/10.1109/IoT-SIU.2018.8519884

[129] Sommer, P. (2017) 'The Future for the Policing of Cybercrime'. In D. Wall (ed.) *Crime and Deviance in Cyberspace* (pp. 8–12). Abingdon: Routledge.

[130] Statista (2023) 'Percentage of Internet Users in Selected Countries Who Have Ever Experienced Any Cyber Crime from November to December 2021'. www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

[131] Stevens, T. and O'Brein, K. (2019) 'Brexit and Cyber Security'. *The RUSI Journal* 164(3): 22–30. https://doi.org/10.1080/03071847.2019.1643256

[132] Tarling, R. and Morris, K. (2010) 'Reporting Crime to the Police'. *British Journal of Criminology* 50(3): 474–490. https://doi.org/10.1093/bjc/azq011

[133] Tcherni, M., Davies, A., Lopes, G. and Lizotte, A. (2016) 'The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?' *Justice Quarterly* 33(5): 890–911. https://doi.org/10.1080/07418825.2014.994658

[134] Tidy, J. (2022) 'NHS IT Supplier Held to Ransom by Hackers'. BBC News, 11 August. www.bbc.co.uk/news/technology-62506039

[135] Van de Weijer, S.G.A. and Leukfeldt, E.R. (2017) 'Big Five Personality Traits of Cybercrime Victims'. *Cyberpsychology, Behavior, and Social Networking* 20(7): 407–412. https://doi.org/10.1089/cyber.2017.0028

[136] Van de Weijer, S.G.A., Leukfeldt, E.R. and van der Zee, S. (2020) 'Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences'. *Policing: An International Journal* 43(1): 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

[137] Victim Support (nd) 'Cybercrime and Online Fraud'. www.victimsupport.org.uk/crime-info/types-crime/cyber-crime/

[138] Wall, D.S. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'. *International Review of Law, Computers & Technology* 22(1-2): 45–63. https://doi.org/10.1080/13600860801924907

[139] Wall, D.S. (2013) 'Policing Identity Crimes'. *Policing and Society* 23(4): 437–460. https://doi.org/10.1080/10439463.2013.780224

[140] Whitty, M.T. (2018) 'Do You Love Me? Psychological Characteristics of Romance Scam Victims'. *Cyberpsychology, Behavior, and Social Networking* 21(2): 105–109. https://doi.org/10.1089/cyber.2016.0729

[141] Wilson, D., Patterson, A., Powell, G. and Hembury, R. (2006) 'Fraud and Technology Crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources'. London: Home Office.

[142] Wilson-Kovacs, D. (2021) 'Digital Media Investigators: Challenges and Opportunities in the Use of Digital Forensics in Police Investigations in England and Wales'. *Policing: An International Journal* 44(4): 669–682. https://doi.org/10.1108/PIJPSM-02-2021-0019

[143] Wirth, A. (2018) 'The Times They Are a-Changin': Part Two'. *Biomedical Instrumentation & Technology* 52(3): 236–240. https://doi.org/10.2345/0899-8205-52.3.236

[144] Wolff, J. (2018) 'The Real Reasons Why Cybercrimes May Be Vastly Undercounted'. Slate, 12 February. https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html

[145] Wooff, A. (2015) 'Relationships and Responses: Policing Anti-Social Behaviour in Rural Scotland'. *Journal of Rural Studies* 39: 287–295. https://doi.org/10.1016/j.jrurstud.2014.11.003

[146] Wooff, A. (2016) '"Soft" Policing in Rural Scotland'. *Policing* 11(2):123–131. https://doi.org/10.1093/police/paw031

[147] Yadav, H., Gautam, S., Rana, A. et al. (2021) 'Various Types of Cybercrime and Its Affected Area'. In J. Tavares, S. Chakrabati, A. Bhattacharya and S. Ghatak (eds) *Emerging Technologies in Data Mining and Information Security* (pp. 305–315). Singapore: Springer. https://doi.org/10.1007/978-981-15-9774-9_30

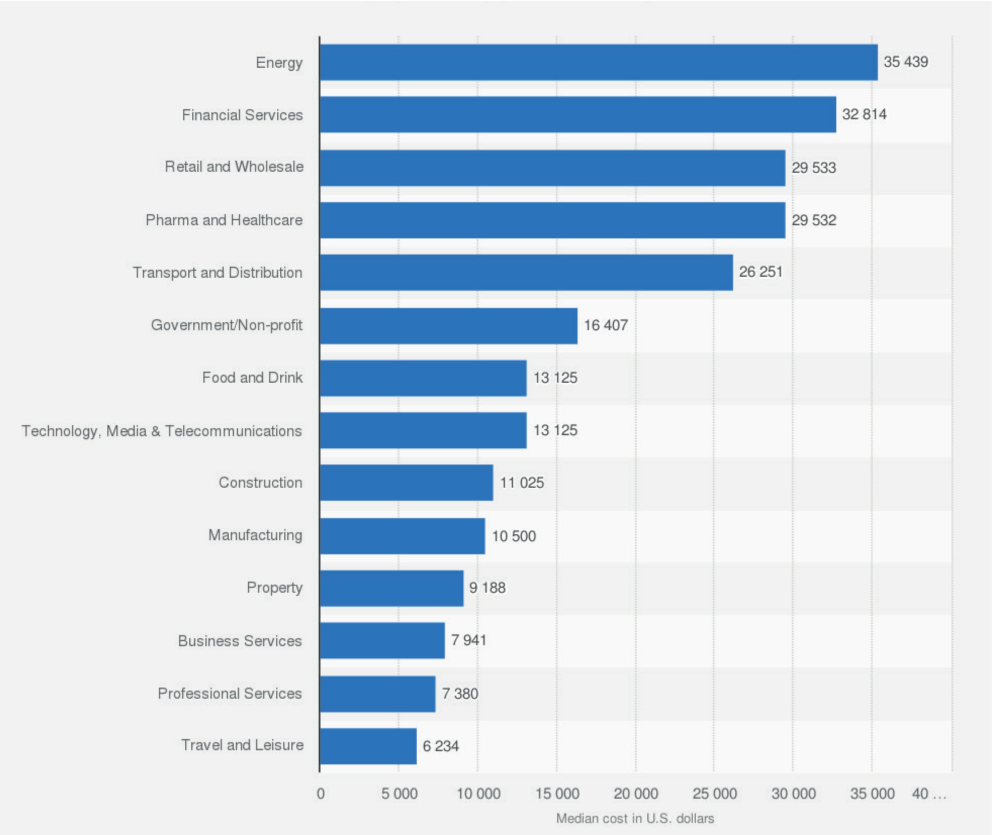
Appendix

Table A1. Annotated analysis of non-UK articles revealed via the systematic method (based on generalisability and/or universality assumptions)

<table>
<tr><th colspan="2">3.1 CYBERCRIME: Annotation of non-UK references</th></tr>
<tr><th>Reference</th><th>References' connection to the UK</th></tr>
<tr><td>[43]</td><td>'COVID-19' and 'older persons' pertain to the UK</td></tr>
<tr><td>[66][111]</td><td>'e-whoring' is a crime occurring globally including in the UK</td></tr>
<tr><td>[128]</td><td>Study focused on 'classification' transferable onto the UK</td></tr>
<tr><th colspan="2">3.2 UK CYBERCRIME VICTIMS: Annotation of non-UK references</th></tr>
<tr><th>Reference</th><th>References' connection to the UK</th></tr>
<tr><td>[13]</td><td>Victims' psychotherapy needs extend onto the UK</td></tr>
<tr><td>[45]</td><td>Victim-blaming may impede cybercrime reporting in the UK</td></tr>
<tr><td>[86]</td><td>An analysis of victims' needs extends onto the UK</td></tr>
<tr><td>[36]</td><td>'Repeat victimisation' pertains to the UK</td></tr>
<tr><td>[135]</td><td>'Big Five Personality traits' model is accepted in the UK</td></tr>
<tr><td>[102]</td><td>Cybercrime and psychiatry have implications for UK patients</td></tr>
<tr><td>[104]</td><td>Young people as a victim group warrant attention in the UK too</td></tr>
<tr><th colspan="2">3.3 CYBERCRIME REPORTING: Annotation of non-UK references</th></tr>
<tr><th>Reference</th><th>References' connection to the UK</th></tr>
<tr><td>[8]</td><td>Important for understanding generalisable reporting issues</td></tr>
<tr><td>[136]</td><td>Comprehensive breakdown of generalisable reporting issues</td></tr>
<tr><td>[4]</td><td>Compares UK to a country with low responsibilisation</td></tr>
<tr><td>[115]</td><td>Extrapolates help-seeking behaviour to the UK context</td></tr>
<tr><td>[7]</td><td>Includes criteria for improving cybercrime reporting applied to UK</td></tr>
<tr><td>[8]</td><td>Undergraduates as a victim group warrant attention in UK too</td></tr>
<tr><td>[70]</td><td>Models voluntary response to cybercrime reporting applied to UK</td></tr>
<tr><td>[58]</td><td>Online counterfeits are a concern for Trading Standards UK</td></tr>
<tr><td>[10][9]</td><td>Models effective reporting applicable to UK</td></tr>
<tr><td>[97]</td><td>Reference to an online platform applicable for research in UK</td></tr>
<tr><td>[41]</td><td>Mentions cybercrime reporting mechanism analogous to UK</td></tr>
<tr><td>[46]</td><td>Pertains to cybercrime reports' structuring useful for UK</td></tr>
<tr><td>[25]</td><td>Online counterfeits are a concern for Trading Standards UK</td></tr>
<tr><td>[126]</td><td>Supplies an automation for spam analysis useful for UK</td></tr>
<tr><td>[127]</td><td>Supplies an automation for phishing detection useful for UK</td></tr>
</table>

[147]	Supplies a cybercrime typology generalisable onto UK
[42]	Cybercrime jurisdiction obstacles impede policing in UK too
[38]	Contrasts cyber expectations vs reality in a way that extends to UK

Figure A1. Average cost of cyber incidents to organisations in the UK as of 2021, by industry



Source: Statista

Figure A2. Prisma 1 & 2 (RQ1: What characterises cybercrime in the UK?)

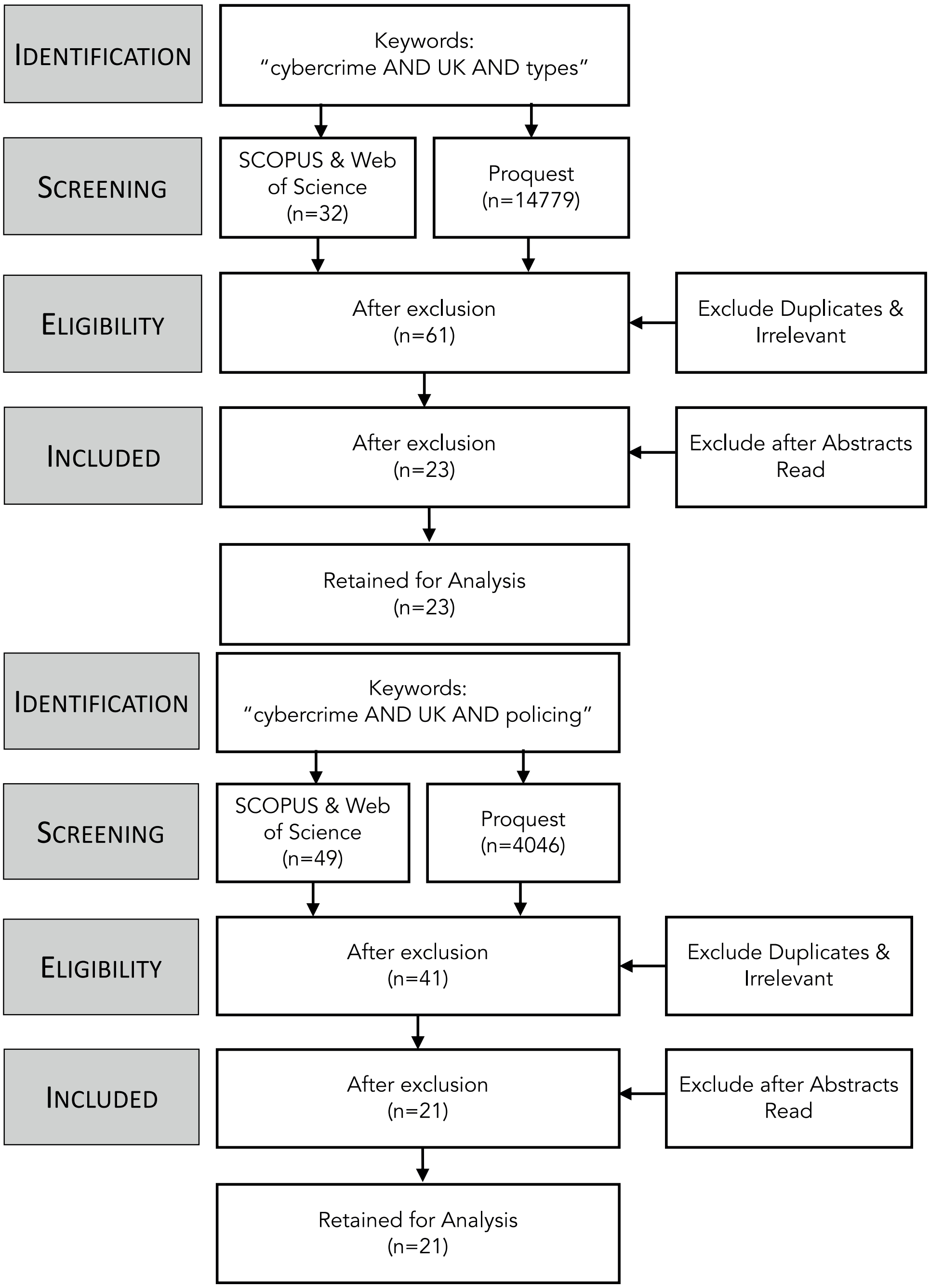

IDENTIFICATION
Keywords: "cybercrime AND UK AND types"
SCREENING
SCOPUS & Web of Science (n=32)
Proquest (n=14779)
ELIGIBILITY
After exclusion (n=61)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=23)
Exclude after Abstracts Read
Retained for Analysis (n=23)
IDENTIFICATION
Keywords: "cybercrime AND UK AND policing"
SCREENING
SCOPUS & Web of Science (n=49)
Proquest (n=4046)
ELIGIBILITY
After exclusion (n=41)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=21)
Exclude after Abstracts Read
Retained for Analysis (n=21)

Figure A3. Prisma 3 & 4 (RQ2: What is known about UK cybercrime victims?)

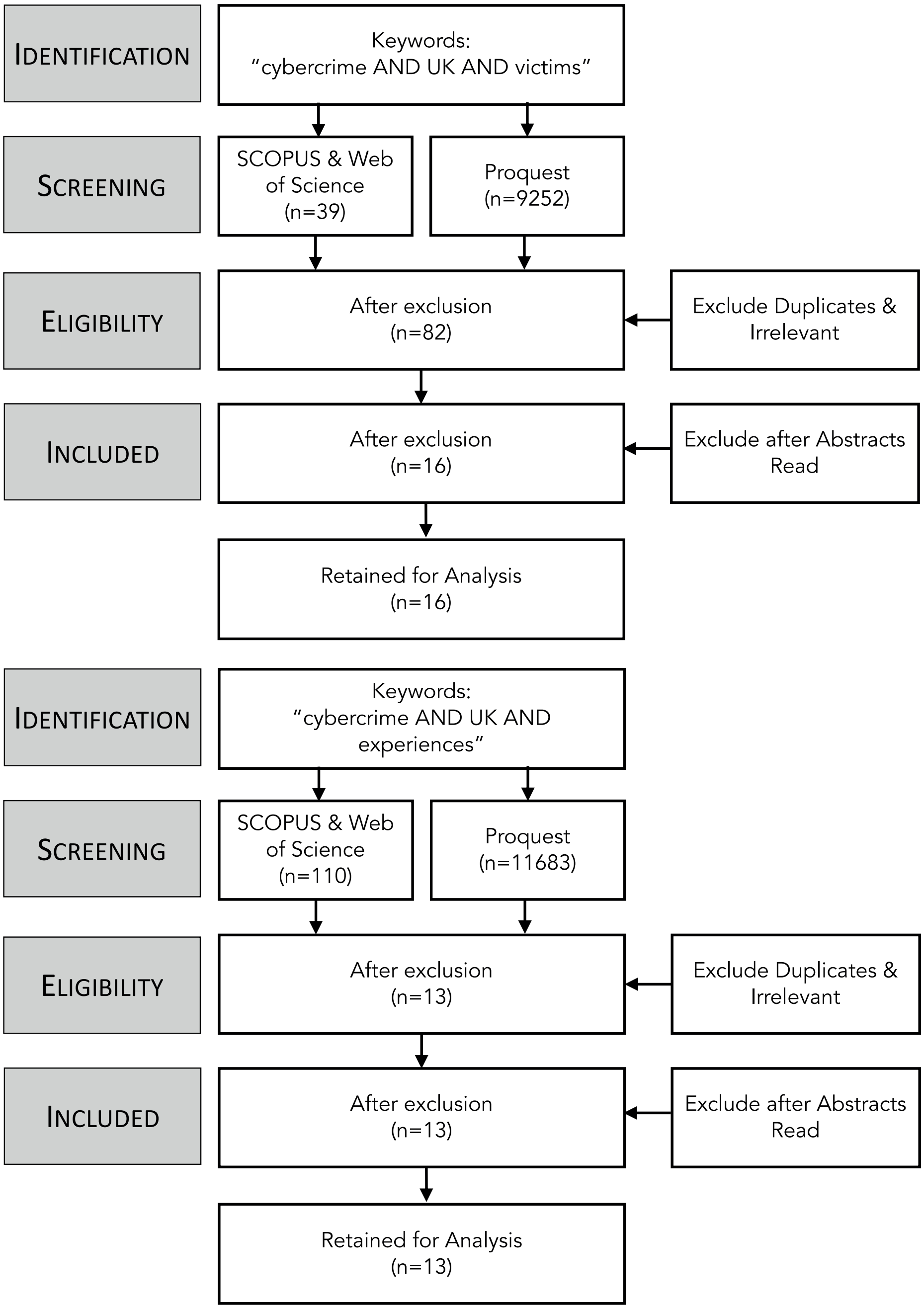
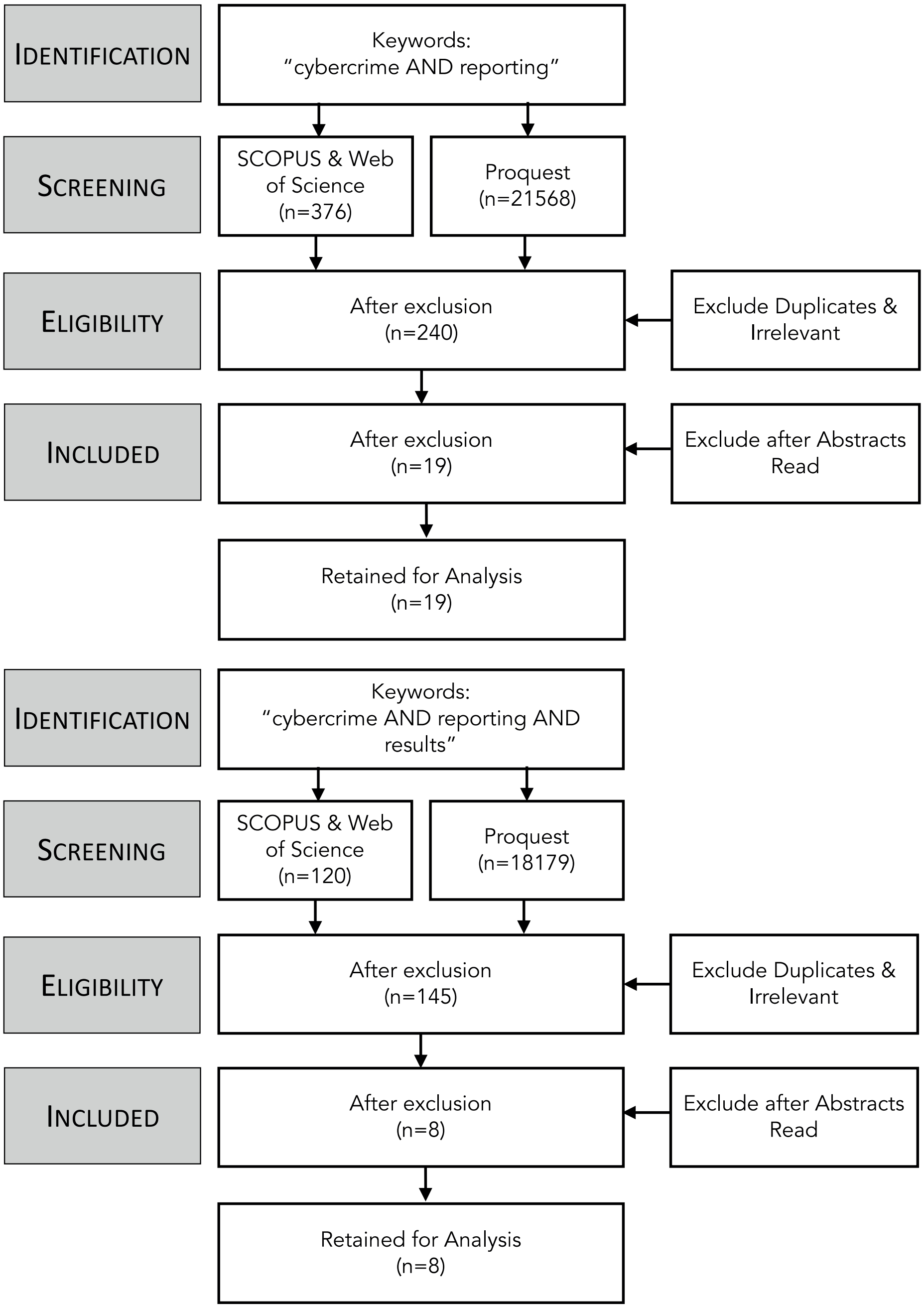

IDENTIFICATION
Keywords: "cybercrime AND UK AND victims"
SCREENING
SCOPUS & Web of Science (n=39)
Proquest (n=9252)
ELIGIBILITY
After exclusion (n=82)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=16)
Exclude after Abstracts Read
Retained for Analysis (n=16)
IDENTIFICATION
Keywords: "cybercrime AND UK AND experiences"
SCREENING
SCOPUS & Web of Science (n=110)
Proquest (n=11683)
ELIGIBILITY
After exclusion (n=13)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=13)
Exclude after Abstracts Read
Retained for Analysis (n=13)

Figure A4. Prisma 5 & 6 (RQ3: What influences and deters cybercrime reporting in the UK)


IDENTIFICATION
Keywords: "cybercrime AND reporting"
SCREENING
SCOPUS & Web of Science (n=376)
Proquest (n=21568)
ELIGIBILITY
After exclusion (n=240)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=19)
Exclude after Abstracts Read
Retained for Analysis (n=19)
IDENTIFICATION
Keywords: "cybercrime AND reporting AND results"
SCREENING
SCOPUS & Web of Science (n=120)
Proquest (n=18179)
ELIGIBILITY
After exclusion (n=145)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion (n=8)
Exclude after Abstracts Read
Retained for Analysis (n=8)

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

The Commonwealth

A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards

Brian Sang YK[1] and Ivan Sang[2]

Abstract

The enactment of Kenya's first comprehensive cybercrime legislation, the Computer Misuse and Cybercrimes Act 2018 ('Cybercrimes Act'), was a significant milestone in laying down legal regulations for cyber-activities. Two international treaty instruments – namely, the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection – were influential in drafting the Cybercrimes Act. Yet some of the provisions of the Cybercrimes Act that establish key definitions and criminal offences are inconsistent with these international treaty standards and in breach of Kenya's Constitution. This article argues that, if not reformed, these defective provisions run the risk of (i) interfering with digital rights and (ii) undermining the efficacy of Kenya's cybercrime law. To systematically make the case for reform, this article comparatively reviews sections of the Cybercrimes Act by juxtaposing them with their equivalents in international treaties and selected national laws. The article proposes amendments to the Cybercrimes Act so as to result in a much more effective regime of cybercrime law in Kenya.

[1] Advocate of the High Court of Kenya; Deputy Director, Administrative Services, County Government of Narok, Kenya. Email: briansang.yk@gmail.com

[2] Senior Researcher, Office of the Deputy Vice-Chancellor Research & Innovation, Strathmore University (Nairobi, Kenya). Email: isang@strathmore.edu

1. Introduction

Like many comparable Commonwealth member countries, Kenya is significantly affected by cybercrime, owing to the increasing reliance on internet-driven services without a corresponding improvement in legal regulations.[3] As a result of the rapid digitisation in Kenya from the late 2000s,[4] the incidence of cybercrime has grown exponentially and it is now estimated to cost the Kenyan economy more than US$210 million annually.[5] Computer systems, devices and tools have been used to fraudulently obtain and launder both public and private funds.[6] Social media networks have also been used to spread hate speech and disinformation, to incite violence and to launch malicious personal or political attacks.[7] Hackers have even leaked classified government records, including a terabyte of private personnel biodata from Kenya's Ministry of Foreign Affairs.[8] Another variant of cybercrime is the insidious use of online platforms to indoctrinate vulnerable Kenyans into violent extremist belief systems, which often results in deadly terrorist activity.[9]

This context underscores Kenya's technological exposure and the extensive impact that cybercrime has on its socio-economic stability and national security.[10] It also underlines the need for a robust cybercrime law in Kenya. As such, the enactment of Kenya's comprehensive cybercrime law, the Computer Misuse and Cybercrimes Act 2018 ('Cybercrimes Act'),[11] was a creditable legislative step in setting out the legal framework for tackling criminal activities online. International treaties – namely the Council of Europe Convention on Cybercrime ('Budapest Convention on Cybercrime')[12] and the African Union Convention on Cyber Security and Personal Data Protection ('Malabo Convention on Cyber Security')[13] – were influential in drafting the Kenyan Cybercrimes Act. Yet, for all the progressive normative contributions of these two international treaties, several provisions of the Kenyan Cybercrimes Act are problematic. This article critiques these defective provisions, which it shows to be inconsistent with both the international treaty standards and Kenya's constitutional rights guarantees.

[3] Kshetri, N. (2019) 'Cybercrime and Cybersecurity in Africa'. *Journal of Global Information Technology Management* 22(2): 77–81.

[4] Rutenberg, I. (2018) *Cyber Law in Kenya*. Philadelphia, PA: Wolters Kluwer.

[5] Serianu (2017), *Kenya Cyber Security Report 2017*. Nairobi: Serianu.

[6] Leftie, P. (2016) 'How Officials Manipulate IFMIS to Steal Public Funds' *Daily Nation*, 27 November. www.nation.co.ke/news/1056-3466304-5fes0sz/index.html

[7] BAKE (2018) *State of the Internet in Kenya 2017*. Nairobi: BAKE.

[8] TESPOK (2017) *Cyber Threats Report 2016*. Nairobi: TESPOK.

[9] Government of Kenya (2016) *National Strategy to Counter Violent Extremism*. Nairobi: Government of Kenya.

[10] UNECA (2014) 'Tackling the Challenges of Cybersecurity in Africa'. Policy Brief. Addis Ababa; UNECA.

[11] Act No. 5 of 2018. This Act is referred to as a comprehensive cybercrime law because it has consolidated and updated the earlier disparate laws that governed improper use of communication devices and computer-related offences. In addition, the Act sets out for the first time an institutional framework for holistic co-ordination at the national level of the detection, prohibition, prevention, response, investigation and prosecution of cybercrimes, as well as for the facilitation of international co-operation in tackling cybercrimes.

[12] ETS No. 185 (entered into force 1 June 2004).

[13] EX.CL/846(XXV) (adopted 27 June 2014).

This article argues that, if not reformed, these defective provisions run the risk of interfering with digital rights and undermining the efficacy of Kenya's cybercrime law. In doing so, it critically assesses the content of Kenya's Cybercrimes Act relating to the criminalisation of cyber-conduct and draws attention to the ways in which the Act can be reformed. This analysis is made in light of a recent judgement in *Bloggers Association of Kenya (BAKE) v Attorney General and 3 Others* in which the High Court of Kenya considered a constitutionality challenge against more than one-third of the sections in the Cybercrimes Act.[14] Although the Court in the *BAKE* judgement held that the challenged sections were constitutionally valid,[15] thereby overturning an earlier court decision to suspend the implicated sections,[16] this article argues that there are cogent reasons to warrant the reform of Kenya's Cybercrimes Act. The article systematically advances the case for the reform of particular provisions of the Act by means of a constructive and comparative critique.

In order to systematically demonstrate the need for amendments to problematic definitions, criminal offences and penalties in Kenya's Cybercrimes Act, this article comparatively reviews the defective sections of the Act by juxtaposing them with their equivalents in the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security. Besides international treaties, the Kenyan Cybercrimes Act is compared with national cybercrime legislation from selected Commonwealth member countries. The national jurisdictions included in this comparative legal analysis are Nigeria, South Africa, New Zealand and the United Kingdom. These jurisdictions were selected on the basis of the high degree of comparability of their respective national cybercrime laws with the Kenyan Cybercrimes Act in terms of the domestic reception of the provisions of the Budapest Convention and, where applicable, the Malabo Convention.

The main aim of this comparative review of Kenya's cybercrime law is twofold: (i) to objectively compare the provisions of the Cybercrimes Act with the legal standards reflecting international best practice; and (ii) to propose concrete amendments to the defective sections of the Act. Structured in three parts, the analysis in this article proceeds as follows.

First, it provides a brief overview of the Kenyan Cybercrimes Act so as to put the subsequent discussion of the current cybercrime law into perspective. Secondly, it evaluates the operative terms and key definitions of Kenya's Cybercrimes Act in light of the international treaty standards in the Budapest Convention and the Malabo Convention. Thirdly, it juxtaposes the substantive offences and sanctions in the Cybercrimes Act vis-a-vis comparable treaty standards in the Budapest Convention and the Malabo Convention. The comparative analysis in the third part also draws on

[14] [2020] eKLR.

[15] Ibid., para. 150.

[16] *Bloggers Association of Kenya (BAKE) v Attorney General and 5 Others* [2018] eKLR, para. 31.

comparable legislation and case law from Nigeria, South Africa, New Zealand and the United Kingdom. The final part synthesises the article's key findings and offers some proposals on the way forward.

2. Overview of the Kenyan Cybercrimes Act

The Kenyan Cybercrimes Act clarifies in its explanatory memorandum the intention of its drafters to 'provide for offences related to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters; and for connected purposes'. Read as a whole, the Kenyan Cybercrimes Act has two closely related aims: (i) to protect the confidentiality, integrity and availability of computer systems, programs and data; and (ii) to facilitate the detection, investigation, prosecution and punishment of cybercrimes. The Act is divided into seven distinct parts and their content is briefly summarised below.

Part I (sections 1–3) sets out the preliminary provisions, including the definition of terms and objects of the Act. Part II (sections 4–13) provides for the establishment and modalities of the National Computer and Cybercrimes Co-ordination Committee. Part III (sections 14–46) stipulates the substantive criminal offences, detailing specific cybercrimes as well as the matching penalties. Part IV (sections 47–56) establishes the relevant investigatory and procedural powers applicable to computer-related offences and cybercrimes, including specific provisions relating to search and seizure of computer data, interception and retention of data, and evidential aspects of such data. Part V (sections 57–65) outlines the framework for international co-operation in relation to the investigation and prosecution of cybercrimes, which often have transnational elements. Part VI (sections 66–69) deals with general provisions, including the priority clause and consequential amendments. Part VII (section 70) specifies how statutory powers conferred by this Act may be delegated.

The provisions of Part III and Part IV are the focus of the present analysis as they jointly stipulate the criminal offences and their penalties, as well as the related investigatory and procedural powers. Before the Act became operational, the Bloggers Association of Kenya (BAKE) filed a petition challenging its constitutionality on the basis that it violated and threatened fundamental rights guaranteed by the Constitution.[17] The petitioners

[17] *BAKE v Attorney General and 5 Others* [2018] eKLR.

specified 26 sections[18] of the Act that cumulatively infringed on the right to privacy, freedom of expression, freedom of media and access to information, the right to a fair trial and equality protections. As regards relief, the petitioners sought conservatory orders to suspend the entry into force of the specified sections of the Act until the merits of the petition were determined.

In May 2018, the High Court per Mwita J granted interim conservatory orders and suspended the operation of the 26 contested sections pending hearing and determination of the petition.[19] That suspension was lifted in February 2020, when the High Court, per Makau J, dismissed the petition.[20] The effect of that judgement was to render the Cybercrimes Act fully effective in its entirety. This article disagrees with that finding but a detailed review of the *BAKE* decision far exceeds the scope of its analysis. Instead, the aim here is to offer a comparative analysis of key definitions and offences in the Cybercrimes Act. Even so, necessary reference will be made to the *BAKE* decision when discussing elements of particular offences in the Cybercrimes Act.

To ensure an objective assessment of the merits and defects of the Kenyan Cybercrimes Act, it is necessary to juxtapose the relevant sections of the Act with selected international treaties and national laws.[21] The discussion in Sections 3 and 4 of this article critiques the selected provisions of the Cybercrimes Act that have the most comparative relevance beyond Kenya. Besides the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security, the Act is juxtaposed with Nigeria's Cybercrimes (Prohibition, Prevention, Etc) Act 2015[22] and South Africa's Cybercrimes Act 2020.[23] Sections 3 and 4 of the article also refer to the case law of the United Kingdom and New Zealand as an aid to the comparative analysis of the Cybercrimes Act.

[18] The challenged sections of the Kenyan Cybercrimes Act are as follows: 5 (composition of the Committee); 16 (unauthorised interference); 17 (unauthorised interception); 22 (false publication); 23 (publication of false information); 24 (child pornography); 27 (cyber-harassment); 28 (cyber-squatting); 29 (identity theft and impersonation); 31 (interception of electronic messages or money transfers); 32 (wilful misdirection of electronic messages); 33 (cyber-terrorism); 34 (inducement to deliver electronic message); 35 (intentionally withholding message delivered erroneously); 36 (unlawful destruction of electronic messages); 37 (wrongful distribution of obscene or intimate images); 38 (fraudulent use of electronic data); 39 (issuance of false e-instructions); 40 (reporting of cyber-threat); 41 (employee responsibility to relinquish access codes); 48 (search and seizure of stored computer data); 49 (record of and access to seized data); 50 (production order); 52 (real-time collection of traffic data); and 53 (interception of content data).

[19] *BAKE v Attorney General and 5 Others* [2018] eKLR, para. 33.

[20] *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 150 (a): 'The Computer Misuse and Cybercrimes Act 2018 is valid and does not violate, infringe or threaten fundamental rights and freedoms.'

[21] Mwiburi, A.J. (2018) *Preventing and Combating Cybercrimes in East Africa: Lessons from Europe's Cybercrime Frameworks*. Berlin: Dunker & Humboldt.

[22] Hereafter 'Nigerian Cybercrimes Act 2015'.

[23] Hereafter 'South African Cybercrimes Act 2020'.

3. Operative terms and key definitions in the Cybercrimes Act

The interpretation of terms is a crucial determinant of the effect of words in the broader scheme of the application of law.[24] An examination of how section 2 of the Kenyan Cybercrimes Act defines certain operative terms yields a mixed report. Some terms are defined in line with international best practice; others are less well defined and may result in problematic outcomes; still others are not defined at all. A few of the definitions that reflect this assessment are discussed below.

One of the key terms used repeatedly in the Kenyan Cybercrimes Act is 'computer system'. section 2 of the Act defines this as consisting in a:

> *physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer includes reference to part of a computer system.*

This definition aligns with the equivalent definition in the Budapest Convention on Cybercrime. Article 1 of the Budapest Convention defines a computer system as 'any device or a group of interconnected or interrelated devices, one or more of which, pursuant to a program, performs the automatic processing of data'. Despite the similarity, though, the definition in section 2 of Kenya's Cybercrimes Act neglects to refer to automatic processing of data as one of the key functions of a computer system. This omission is a significant shortcoming as the Act then fails to take account of developments in artificial intelligence, to indicate that automatic processing of data will be the predominant element of computer systems as automated capabilities continue to advance.[25] Current trends in social media technology that make it possible to leverage automatic data processing and the rapid evolution of big data analyses illustrate these developments.[26]

The definition of 'computer system' in the Malabo Convention on Cyber Security (in article 1) is overly technical and may not provide meaningful guidance for amending the Kenyan Cybercrimes Act.[27] In contrast, the equivalent definition in the Budapest Convention on Cybercrime presents a more pliable model that can be adopted with advantage in Kenya. It is also relevant that the Nigerian Cybercrimes Act 2015 (section 42) and South Africa's Cybercrimes Act 2020 (section 1(1)) both implicitly refer to the capability of automatic

[24] Hutton, C. (2009) *Language, Meaning and the Law*. Edinburgh: Edinburgh University Press.

[25] Zou, W., Xu, D. and Yu, J. (2012) 'Embedded Vision Positioning System Based on ARM Processor' in Xu, D. (ed.) *Embedded Visual System and Its Application on Robots*. Bentham Books.

[26] Roosendaal, A., Kert, M., Lyle, A. and Gasper, U. (2016) 'Data Protection Law Compliance for Cybercrime and Cyberterrorism Research', in B. Akhgar and B. Brewster (eds) *Combating Cybercrimes and Cyberterrorism: Challenges, Trends and Priorities*. Springer; Council of Europe (2010) 'The Protection of Individuals with Regard to Automatic Processing of Data in the Context of Profiling'. Recommendation CM/Rec(2010)13, adopted 23 November.

[27] Jamil, Z. (2016) 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime'. Technical Report for GLACY+.

processing of data in their respective definitions of a computer system. This reflects a modicum of consensus on the need to include the automatic data processing function in the definition of computer systems.

The Kenyan Cybercrimes Act also refers repeatedly to 'authorised person' in reference to individuals variously empowered to exercise powers or undertake such procedures as may be necessary for effective detection, investigation and prosecution of cybercrimes.[28] Yet this term is defined as 'a person designated by the Cabinet Secretary responsible for matters relating to national security by notice in the Gazette' to give effect to the investigative procedures outlined in Part IV of the Act (Section 2). By failing to specify clearly the individuals who may be regarded as authorised persons, the Cybercrimes Act gives too much discretion to the cabinet secretary.

This is problematic in light of the coercive and intrusive powers that part iv of the act gives the cabinet Secretary. Previous experience in Kenya as well as in other comparable jurisdictions shows a tendency for state officials to abuse such powers.[29] It is therefore advisable in the context of a future law reform process that the term 'authorised persons' be more specifically defined and limited so as to safeguard against the risk of unilateral and unchecked expansion of police powers by the minister.

4. Criminal offences and sanctions in the Cybercrimes Act: a comparative critique

The Kenyan Cybercrimes Act provides, in Part III, for the criminalisation of 27 offences. This far exceeds the number of offences in the Budapest Convention on Cybercrime,[30] which, together with its Protocol,[31] criminalises a total of 14 offences. It also surpasses the number of offences in the Malabo Convention on Cyber Security, which lists 13 offences. This greater number of offences results from splitting cybercrimes to highlight specific criminalised conduct as well as from the criminalisation of conduct relating to the fraudulent or wrongful use of electronic data. Although this approach is not without some merits, the overall impact of stipulating many offences leads to unnecessary duplication of offences.

[28] Sections 48(1), 48(4), 49(2), 49(3), 50(1), 51(1), 51(7), 52(1), 53(1), 53(2) and 54(2).

[29] *Law Society of Kenya v Inspector General Kenya National Police Service and 3 Others* [2015] eKLR; *Coalition for Reform and Democracy (CORD) and 2 Others v Republic of Kenya and Others* [2015] eKLR. For a comparative account on how this power has tended to be abused in other jurisdictions, see Omotubora, A. (2019) 'Old Wine in New Bottles: Critical and Comparative Perspectives on Identity Crimes under the Nigerian Cybercrime Act 2015' *African Journal of International and Comparative Law* 27(4): 609-628.

[30] Clough, J. (2014) 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation'. *Monash University Law Review* 40(3): 698.

[31] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (28 January 2003).

Unlike the Budapest Convention and the national cybercrime laws of some states,[32] the Kenyan Cybercrimes Act does not explicitly classify its offences into distinct categories of cybercrimes. In the Budapest Convention, these include (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer-related offences; (iii) content-related offences; and (iv) offences related to criminal infringements of copyright and other related rights (Chapter II, Section 1, Titles 1–4). Nonetheless, as with the Malabo Convention on Cyber Security, a closer review of the structure of Part III of the Kenyan Cybercrimes Act shows that the criminalised offences are arranged approximately into the four categories of cybercrime. For this reason and in the interests of brevity, the comparative analysis of the offences established in the Kenyan Cybercrimes Act is based broadly on these four types of cybercrime.

4.1 Unauthorised access

Section 14(1) of the Kenyan Cybercrimes Act criminalises unauthorised access, which entails intentional infringement of security measures with intent to gain unlawful access to a computer system, and with the knowledge that such access is unauthorised.[33] This provision is welcome to the extent that it specifies the material element of the offence that must be satisfied before criminal liability attaches: it requires the actual or attempted breach of security measures of a computer system. However, it offers no elaboration of the acts that constitute gaining or securing access. This is an omission that may present some difficulty when adjudicating alleged cybercrimes. By contrast, section 2(2)(a–d) of the South African Cybercrimes Act 2020 provides a detailed exposition of the instances in which it can accurately be alleged that a person has intentionally and unlawfully secured access to data, a computer program, a computer data storage medium and a computer system. This provides an instructive basis for amending the text of section 14(1) to strengthen its currently defective material element.

Also, the wording of the mental element of the offence of unauthorised access is inelegant, legally defective and inadequate. Although section 14(1) of the Kenyan Cybercrimes Act seems consistent with article 29(1) of the Malabo Convention on Cyber Security and article 2 of the Budapest Convention on Cybercrime, it falls short of the legal standards in these international treaty instruments.[34] In particular, it fails to specify the qualitative nature of intent as either fraudulent or dishonest, and it does not disclose the motive of such access. Section 14(3) of the Act is also defective because it distorts the relevance of intent as a core element of the crime and renders it irrelevant what the criminal motive or objective is.

[32] See Clough, J. (2015) *Principles of Cybercrime*. Cambridge: Cambridge University Press.

[33] 'A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.'

[34] Jamil (2016) 'Comparative Analysis'.

A constructive method of illustrating the deficiency of section 14 of the Cybercrimes Act is to juxtapose it with an equivalent provision that is more comprehensively drafted. Article 2 of the Budapest Convention on Cybercrime criminalises illegal access to a computer system and also imposes an obligation on each of the states parties to:

> *establish as criminal offences, under its domestic law, when committed intentionally, the access to the whole or any part of the computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

Like section 14(1) of the Kenyan Cybercrimes Act, the above provision specifies the mental elements of the offence: it must be committed 'intentionally' and 'without right'. However, unlike section 14(1), article 2 of the Budapest Convention further specifies that the nature of the intent must be dishonest. More importantly, it draws a connection between these mental elements and the underlying criminal objective by clarifying, in inclusive language, that the ultimate motive of the illegal access should be to obtain computer data or for other dishonest ends. It is thus recommended that section 14 of the Kenyan Cybercrimes Act be amended to better clarify the specific mental elements of the dishonest intent to gain access to a computer system for the purpose of obtaining computer data, or to commit or facilitate the commission of another offence.

Despite its imperfect drafting, section 14 of the Kenyan Cybercrimes Act creditably seeks to define what constitutes 'unauthorised access'. Section 14(2)(a–b) states that access by a person to a computer system is unauthorised if that person (i) is not 'entitled to control access of the kind in question to the program or data'; or (ii) 'does not have consent from any person who is entitled to access the computer system through any function to the program or data.' This makes it easier for law enforcement and judicial authorities to distinguish between lawful and unlawful access, and is thus a laudable merit of the Kenyan Cybercrimes Act.

4.2 Access with intent to commit a further offence

Section 15(1) of the Kenyan Cybercrimes Act criminalises unauthorized access 'with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person'. Section 15(2) additionally stipulates that it is immaterial that the further offence was committed at the time when the unauthorised access was secured or at any other time. For an offence that exposes individuals upon conviction to a prison term of up to 10 years or a fine of up to Ksh 10 million, section 15 establishes a broad offence that fails to take sufficient account of the seriousness of the criminalised conduct or its temporal scope. The adverse implication here is that its penal regime does not distinguish between serious and less serious offences. This is an acute legislative flaw that calls for urgent reform.

Besides failing to criminalise only intent to commit a specific act of serious gravity, offences of the kind outlined in section 15 of the Kenyan Cybercrimes Act are not recognised in the Budapest Convention on Cybercrime or the Malabo Convention on Cyber Security. This omission may suggest that the conduct criminalised in section 15 of the Kenyan Cybercrimes Act could effectively be addressed within the offence of unauthorised access. Even so, the legislation from comparable jurisdictions indicates recognition of the need for a distinct offence of unlawful access with intent to commit specific criminalised conduct.

Although not identical in wording to the equivalent Kenyan provision, section 36 of the Nigerian Cybercrimes Act 2015 criminalises gaining access, with the intent to defraud, to any device, attachment, email or website to obtain credit card details.[35] In contrast to both the Kenyan and the Nigerian provisions, section 4 of the South African Cybercrimes Act 2020 criminalises only the unlawful and intentional securing of access. The most commendable aspect is that it crucially relates the criminalised act to other offences, including unlawful acts in respect of software (section 2(2)(c)) and the unlawful dealing in passwords, access codes or similar data or devices (sections 7(1) and 7(2)).

This suggests that the drafters of section 15 of the Kenyan Cybercrimes Act likely envisaged the types of offences described in the equivalent cybercrime laws of South Africa and Nigeria, but the text of the resulting provision falls short of the requirements of specificity and legal certainty.[36] To remedy this defect, it is proposed that section 15(1) of Kenya's Cybercrimes Act also criminalise unauthorised access that is designed or intended to facilitate a specified range of offences. Guided by the imperative of legal certainty, it is further proposed that an inclusive list of further offences to which penalty applies on conviction be enumerated in the amended provision. The cross-referencing technique used in the South African Cybercrimes Act 2020 is also highly recommended. On the same rationale, section 15(2) of Kenya's Cybercrimes Act, which makes irrelevant the gravity or timing of the offence, should be struck out altogether.

4.3 Unauthorised interference

Section 16(1) of the Kenyan Cybercrimes Act subjects any person who intentionally and without authorisation carries out any act that causes unauthorised interference to a computer system, program or data to a penalty, on conviction, of a fine not exceeding Ksh 10 million[37] or to imprisonment for a term not longer than five years, or to both. In the

[35] Chakwi, M., Darwish, A., Khan, M.A. and Tyagi, S. (2015) 'Cybercrime, Digital Forensics and Jurisdiction'. *Studies in Computational Intelligence*. Springer.

[36] *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33: 'There are two principles: no one should be punished under a law unless it is sufficiently clear and certain to enable him to know what conduct is forbidden before he does it; and no one should be punished for any act which was not clearly and ascertainably punishable when the act was done.'

[37] Approximately US$82,045.

BAKE case, this section was the subject of a constitutionality challenge on the ground that it does not specify the element of *mens rea* and thus risks criminalising innocent conduct.[38]

Section 16(2)(a–b) of the Kenyan Cybercrimes Act defines unauthorised interference as action causing interference perpetrated by a person who (i) is 'not entitled to cause that interference' or (ii) 'does not have consent to interfere from a person who is so entitled.' In the event that unauthorised interference results in significant financial loss to any person, threatens national security, causes physical injury or death to any person or threatens public health or public safety, section 15(3) of the Act imposes much stiffer penalties on conviction: a fine not exceeding Ksh 20 million or imprisonment for a term not exceeding 10 years, or both.

While the provisions of section 16 of the Kenyan Cybercrimes Act address important aspects of cybercrime regulation, they are deficient in ways that can best be illustrated by comparison. Section 16(1) of the Act criminalises unauthorised interference without relating it to the corresponding degree of harm. This runs into the difficulty of creating a vague offence that fails to satisfy the requirement of legal certainty.[39] By contrast, article 5 of the Budapest Convention on Cybercrime, which criminalises the equivalent offence of system interference, refers to the requisite threshold of harm using the words 'serious hindering'.[40] This indicates a high level of seriousness of damage or impairment.[41] To strengthen section 16 of Kenya's Cybercrimes Act, it is proposed that its content be modified by specifying the degrees of harm outlined in section 16(3)[42] in section 16(1), and by enunciating the material element of the offence as either serious damage or impairment of the functionality of a computer system.

A suitable model to guide the amendment of section 16 of the Kenyan Cybercrimes Act is section 5 of the South African Cybercrimes Act 2020. That provision helpfully explains that interference with a computer data storage medium, a computer program or a computer system means to permanently or temporarily interrupt or impair the functionality or to render the data or computer program ineffective.

[38] *BAKE v Attorney General and 3 Others* [2020] eKLR, paras 87 and 89.

[39] This standard, which applies across common law jurisdictions, was clarified by the United Kingdom House of Lords in *R v Rimmington and Goldstein* [2006] 1 AC 549, para 33.

[40] 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.'

[41] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*. Strasbourg: Council of Europe.

[42] 'A person who commits an offence under subsection (1) which – (a) results in a significant financial loss to any person; (b) threatens national security; (c) causes physical injury or death to any person; or (d) threatens public health or public safety, is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.'

4.4 Unauthorised interception

Section 17(1) of the Kenyan Cybercrimes Act is formulated in a manner similar to section 16(1);[43] it criminalises the conduct of a person who intentionally and without authorisation carries out any act that, directly or indirectly, intercepts or causes the interception of transmission of data to or from a computer system. In the *BAKE* case, the petitioners contended that section 17(1) of the Act created an offence without specifying the element of *mens rea* and was therefore unconstitutional.[44] Section 17(2) provides enhanced sanctions for identical offences to those in section 16(3).[45] As with section 16, the provisions of section 17 establish an unduly broad range of offences. Thus, to avoid duplication, the comments made above[46] on the need for specificity in section 16 apply in like manner to the corresponding provisions of section 17.

However, a notable aspect of unauthorised interception as set out in the Kenyan Cybercrimes Act that requires special mention is the content of the offence. Compared with international instruments on cybercrime,[47] the offence of unlawful or illegal interception is deficient and a number of crucial elements of the offence are omitted.[48] To illustrate this, it is instructive to examine the text of article 3 of the Budapest Convention on Cybercrime, which establishes the equivalent offence of illegal interception and calls for its criminalisation:

> *when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

These detailed provisions indicate that, as presently constituted, section 17 of the Kenyan Cybercrimes Act is incomplete and imprecise.

To remedy these shortfalls, it is recommended that section 17 of Kenya's Cybercrimes Act be amended to criminalise only the interception of 'non-public' transmissions of computer data made possible by use of 'technical means'. Also advocated is the inclusion in section 17(1) of an offence relating to electromagnetic emissions, which are not 'data' in the technical sense.[49] However, as clarified in the explanatory report to the Budapest Convention, because 'data can be reconstructed from such emissions,' the dishonest and intentional interception of data from electromagnetic emissions from a computer system should be included within the ambit of section 17(1).[50] Section 17(1) should further

[43] See Section 4.3 of this article.
[44] *BAKE v Attorney General and 3 Others* [2020] eKLR, paras 87 and 89.
[45] See Section 4.3 of this article.
[46] See Section 4.3 of this article.
[47] Budapest Convention on Cybercrime article 3; Malabo Convention on Cyber Security article 29(2)(a).
[48] Budapest Convention on Cybercrime article 5; Malabo Convention on Cyber Security article 29(1)(d).
[49] Clough (2015) *Principles of Cybercrime*.
[50] Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*, para. 57.

incorporate the *mens rea* element of dishonest intent and specify that interception must be in reference to transmission of data between one computer system linked to another. This would render sub-sections 17(2), (3) and (4) redundant and subject to removal.

The text of section 3 of the South African Cybercrimes Act 2020, which criminalises unlawful interception of data, is a suitable model on which the revision of the equivalent Kenyan provision can be based. The reason for this is that, unlike section 17 of the Kenyan Cybercrimes Act, it includes all the essential elements of the offence of unlawful or illegal interception. In addition, section 3 of the South African Cybercrimes Act 2020 aligns with the international standards in the Budapest Convention on Cybercrime.

4.5 Illegal devices and access codes

Section 18(1) of the Kenyan Cybercrimes Act envisages the criminal liability of anyone who knowingly 'manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data' designed or primarily adapted to commit a cybercrime. Section 18(2) extends criminal liability to anyone who knowingly receives or is in possession of such illegal devices or programs as a result of, or with the intention to use it to commit, an offence under the Act. The wording of section 18(1) of Act is unsatisfactory as it uses the *mens rea* standard of 'knowingly' in relation to dynamic technologies with dual-use capabilities that can equally be used for lawful or unlawful purposes.[51]

This standard therefore unwisely criminalises an overbroad category of activities and exposes a wide range of actors (virtually the entire chain, from manufacturer, to distributor, to retailer, to end-user) to criminal liability, as all may have knowledge of the potential dual uses of such technology. This clearly highlights the pernicious implications of expansively criminalising the use of computer software and devices.[52] An analogy that can illustrate the adverse effect of section 18 of the Kenyan Cybercrimes Act may be drawn from manufacturers, wholesalers, retailers and users of glass products: while all parties know that broken glass may be used as a weapon, this does not in itself justify criminalising dealing in glassware.

A more appropriate legal standard of criminal intent should therefore be substituted for 'knowingly' in order that the criminality of illegitimate use of dual-use tools should turn exclusively on proof of the subjective intent to commit a cybercrime.[53] It is proposed that 'intentionally' is a much better-suited standard as it clearly reflects the deliberation between the actor and the crime. In its amended form, therefore, section 18 of the Kenyan Cybercrimes Act should criminalise intentional possession without justifiable cause and use of illegal devices and codes for the purpose of committing a cybercrime.

[51] Day, E. and Bryant, R. (2016) 'Law and Digital Crime', in R. Bryant (ed.) *Policing Digital Crime*. Abingdon: Routledge.

[52] Sommer, P. (2006) 'Criminalizing Hacking Tools'. *Digital Investigations* 3(2): 68-72.

[53] Clough (2015) *Principles of Cybercrime*.

Another possible descriptor of the specific intent element of this offence may be 'unlawfully and intentionally', as used in the South African Cybercrimes Act 2020. Article 6 of the Budapest Convention on Cybercrime, which establishes the equivalent offence of misuse of devices, criminalises similar conduct when it is 'committed intentionally and without right'. The text of article 6 of the Budapest Convention, unlike that in the Malabo Convention on Cyber Security (in article 29(1)(h)), is better placed to offer a model for amending section 18(1) of the Kenyan Cybercrimes Act. Section 7 of the South African Cybercrimes Act 2020 is also an instructive basis for guiding legal reform because, unlike its Kenyan equivalent, it specifically criminalises the possession and use of computer devices and tools for purposes of committing particular prohibited acts.

It is notable that section 18(3) of the Kenyan Cybercrimes Act provides safeguards by exculpating as non-criminal a narrow set of conduct relating to the possession and use of passwords and access codes. These include any act intended for the authorised training, testing or protection of a computer system; or the use of a computer program or password or access code in compliance or accordance with a lawfully issued judicial order. This is a prudent provision that immunises a crucial component of the work of information and communication technology professionals and system administrators – testing the soundness of computer security systems, which invariably entails trying to breach firewalls.[54] A provision that draws a clear distinction between, on the one hand, legitimate and protected conduct and, on the other, illegal and punishable conduct is certainly well conceived.

Closely related to section 18 of Kenya's Cybercrimes Act is section 19, which criminalises the unauthorised disclosure of any password, access code or other means of gaining access to any program or data held in any computer system. The operative elements of this offence are that such disclosure should be made 'knowingly' and 'without authority'. Problems related to the use of 'knowingly' as a standard of specific intent have been stated above and will not be repeated.[55] As for the element of 'without authority', this presents a serious challenge to effective enforcement because it is not defined in the Kenyan Cybercrimes Act. The combined effect of these two elements is that section 19 of the Act will criminalise legitimate conduct because, unlike section 18(3), it does not immunise training, testing or protection of computer systems. Nor does it immunise other related and legitimate activities that may be facilitated by the disclosure or sharing of passwords and access codes. This is a weakness of the Kenyan Cybercrimes Act that needs to be reconsidered.

[54] 'Many items of this nature [i.e. passwords and access codes] are "dual use", and widely used by security professionals and system administrators. For example, penetration testing devices are used to detect security weaknesses, but may also be used by hackers as a way of gaining unauthorised access' (Clough, 2015, *Principles of Cybercrime*: p.135).

[55] See Sections 4.3 and 4.4 of this article.

Some useful insight to guide the amendment of section 18 of the Kenyan Cybercrimes Act may be drawn from the South African equivalent. Section 7 of the South African Cybercrimes Act 2020 criminalises the unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data. The elements of this offence in the South African Cybercrimes Act 2020 are that a person unlawfully and intentionally acquires, possesses, provides to another person or uses the password, access code or similar data for purposes of committing a cybercrime (section 7(1)). As well as clearly articulating the elements, the South Cybercrimes Act offers a basis to exculpate certain legitimate action that may constitute the offence. Section 7(2) immunises such legitimate conduct where a person found in possession of a password or access code is able to give 'a satisfactory exculpatory account of such possession'.

4.6 Offences involving a protected computer system

Section 20(1) of the Kenyan Cybercrimes Act establishes an enhanced penalty for (i) unauthorised access, (ii) access with intent to commit a further offence, (iii) unauthorised interception and (iv) unauthorised interference, where these are committed on a 'protected computer system'. Such systems are defined in section 20(2)(a–f) of the Act as those 'used directly in connection with, or necessary for' national security; protecting the existence or identity of a confidential source of information related to law enforcement; provision of services related to communication infrastructure and electronic banking or financial services; protection of public safety and emergency services; provision of national registration systems; or such other systems as may be designated by the cabinet secretary relating to information and communication technology.

These examples are imprecisely worded, with the result that the narrow category of protected computer systems may become too expansive for efficient judicial management. It therefore becomes impossible for individuals to engage in ordinary computer-related activity without the anxiety of being at risk of onerous legal liability. For this reason, among others, it is proposed that section 20(2) of the Kenyan Cybercrimes Act be amended and formulated along the lines of comparable national cybercrime laws that protect critical information infrastructure.[56] In addition, it is recommended that the words 'protected computer system' be replaced with 'critical information infrastructure', which communicates clearly the national importance of the specified computer systems and the seriousness of any attacks on them.[57]

Nigerian cybercrime law may be instructive in this regard. Section 5(1) of the Nigerian Cybercrimes Act 2015 provides, *inter alia*, that any person who intentionally commits any offence punishable under the Act against any critical national information infrastructure is liable, on conviction, to imprisonment for a term not exceeding 10 years without

[56] Clough (2015) *Principles of Cybercrime*.

[57] Reich, P. (2012) 'To Define or Not to Define: Law and Policy Conundrums for the Cybercrime, National Security, International Law and Military Law Communities', in P. Reich and E, Gelbstein (eds) *Law, Policy and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*. Hershey, PA: IGI Global.

the option of a fine.[58] What is more, this Act defines 'critical national information infrastructure' as certain designated computer systems, networks, programs and traffic computer data, the destruction of which would have a debilitating impact on national security, public health and safety, or a combination of these (section 42). A more concise and better-drafted definition of critical cyber-infrastructure is found in the text of the equivalent United States legislation that inspired the Nigerian cybercrime law:

> *In this section, the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[59]

Although the United States and Nigerian statutes do not identify precisely what constitutes critical national information infrastructure, they are instructive to the extent that both advert to a high threshold of harm – incapacitation or destruction of such critical cyber-infrastructure that can result in a 'debilitating impact'. This, unlike the position in section 20 of Kenya's Cybercrimes Act, comports with the standard of serious damage or impairment reflected in international best practice.[60] The implication here, which is simultaneously a recommendation towards amending section 20 of Kenya's Cybercrimes Act, is that only serious impairment or loss should attract the enhanced penalties.

The South African Cybercrimes Act 2020 arguably offers more precise guidance on what amounts to critical national cyber-infrastructure. Section 11 criminalises as an 'aggravated offence' interception, interference, misuse of computer data or computer system in relation to a restricted computer system. The phrase 'restricted computer system' is functionally equivalent to 'critical national infrastructure' as used in the Nigerian Cybercrimes Act, and is defined as:

> *any data, computer program, computer, computer data storage medium or computer system –*
>
> *i. under the control of, or exclusively used by –*
>
> *ii. (aa) a financial institution; or*
>
> *iii. (bb) an organ of state as set out in section 239 of the South African Constitution, including a court; and*
>
> *iv. which is protected by security measures against unauthorized access or use.*

[58] Okoh, J. and Chukwueke, E. (2016) 'The Nigerian Cybercrime Act 2015 and Its Implications for Financial Institutions and Service Providers'. *Financier Worldwide*, July.

[59] 42 US Code § 5195c.

[60] Jamil (2016) 'Comparative Analysis'.

Another aspect of the provisions for enhanced offences against protected computer systems in the Kenyan Cybercrimes Act that call for reform is the high degree of ministerial discretion. Section 20(2)(f) of the Kenyan Cybercrimes Act empowers the cabinet secretary responsible for matters relating to information, communication and technology to designate as a protected computer system in 'the manner or form as [he/she] may consider appropriate' any other computer system that he or she regards fit. The formulation of this provision establishes a broad and inexact discretion because it offers no guidance on the categories of systems that may possibly be included in the class of protected computer systems. Apart from being open to governmental abuse, this lack of guidance may diminish the heightened status of protection accorded to critical national information infrastructure.

Accordingly, it is recommended that section 20(2)(f) of the Kenyan Cybercrimes Act be amended to better define the category of protected computer systems and specify clear limits on ministerial discretion. In particular, there should be a requirement that the cabinet secretary designate, on the basis of justifiable reasons, that a particular computer system or network is crucial in protecting a vital national interest.[61] This recommendation for legislative reform coheres with the requirement in article 47 of the Kenyan Constitution to supply reasons for administrative decisions that may affect fundamental rights or other legal interests.

Commentators on the legislative antecedents of the Kenyan Cybercrimes Act observed that the provisions equivalent to section 20 of the current Act were unnecessarily duplicative and could be omitted by means of more careful legal drafting.[62] They suggested two aspects of this preferred approach. First, it was proposed that, if the intentionality requirements in sections 14, 15, 16 and 17 of the Act were heightened, the additional penalties in section 20 could be rendered redundant. Second, it was argued that, if the specification of the relevant degrees of harm were included and targeted references were made to a better defined set of critical national information infrastructure, section 20 of the Act again could be rendered unnecessary. This is a prudent approach that is in accordance with the public policy objective of having fewer yet more detailed cybercrimes. It is thus endorsed as a recommended amendment to Kenya's Cybercrimes Act.

4.7 Computer forgery and fraud

Section 25(1) of the Kenyan Cybercrimes Act criminalises the conduct of any person who 'intentionally inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.' The text of this provision is derived, almost word for word, from article 7 of the Budapest

[61] Article 19 (2018) *Kenya: Computer and Cybercrimes Bill 2017*. London: Article 19.

[62] Ibid.

Convention on Cybercrime,[63] and it is also substantially the same as article 29(2)(b) of the Malabo Convention on Cyber Security.[64] However, section 25(2) of Kenya's Cybercrimes Act differs in a key respect from the equivalent provisions in these international treaties; it establishes enhanced penalties if the computer-related forgery is committed 'dishonestly or with similar intent—(a) for wrongful gain; (b) for wrongful loss to another person; or (c) for any economic benefit for oneself or for another person.'

In contrast, both the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security require as an essential element of the offence 'an intent to defraud, or similar dishonest intent, before criminal liability attaches.'[65] This indicates that section 25(2) of the Kenyan Cybercrimes Act unnecessarily creates heightened criminal sanctions for offences that should be encompassed under section 14(1) of the Act. To better serve public policy objectives and to comply with the *ultima ratio* rule of minimal criminalisation,[66] section 14(1) of the Act should be amended to incorporate 'dishonest intent' as a core element of the offence of computer-related forgery, while the fraudulent intent can be an example of such dishonesty.

Section 26(1) of the Kenyan Cybercrimes Act, which is closely related to section 25(1), criminalises computer fraud. It provides that a 'person who, with fraudulent or dishonest intent', unlawfully gains an economic benefit for himself/herself or another person, or occasions a loss to another person, through the use of a computer system, program or data, commits an offence. With appropriate adaptation, the text of section 26(1) of the Act presents a viable model for moulding the proposed changes to section 25(1) of Kenya's Cybercrimes Act.

Even so, section 26(2) of the Kenyan Cybercrimes Act is not exactly a model of clarity. Its description of the 'means' by which computer fraud may be carried out is overly complicated and long-winded when juxtaposed with the more concisely formulated equivalent provisions of the Budapest Convention on Cybercrime (article 8) and the Malabo Convention on Cyber Security (article 29(2)(d)). The latter provisions, which reflect international best practice standards, regard as sufficient that national cybercrime laws criminalise gaining of any benefit or causing loss to another person through means of any

[63] 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.'

[64] 'State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: … Intentionally input, alter, delete or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.'

[65] Jamil (2016) 'Comparative Analysis'.

[66] Viano, E.C. (2017) 'Cybercrime: Definition, Typology, and Criminalization', in E.C. Viano (ed.) *Cybercrime, Organised Crime, and Societal Responses: International Approaches*. Amsterdam: Springer.

interference with the functioning of a computer system. Thus it is recommended that section 26 be simplified to bring it in line with article 29(2)(d) of the Malabo Convention on Cyber Security and article 8 of the Budapest Convention on Cybercrime.

4.8 Cyber-harassment

Section 27(1) of Kenya's Cybercrimes Act criminalises cyber-harassment and is one of the provisions whose constitutionality was challenged in the *BAKE* case.[67] The *BAKE* petitioners submitted that section 27 criminalised speech on grounds that had no proximate relationship to the legitimate grounds for limitation of free speech;[68] and further, that in doing so, it used vague and subjective phrases such as 'apprehension of fear or violence' and 'indecent or grossly offensive'.[69] The offence of cyber-harassment is described in section 27(1) of the Act as consisting in the action of:

> *A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone known to that person … if they know or ought to know that their conduct:*
>
> *a. is likely to cause those persons apprehension or fear of violence to them or damage or loss on that person's property; or*
>
> *b. detrimentally affects that person; or*
>
> *c. is in whole or part, of an indecent or grossly offensive nature and affects the person.*

This definition is problematic for two reasons. First, it is unduly complex, legally imprecise and, in turn, unclear in its meaning. It is notable, however, that the effects specified in clauses (a) and (b) of section 27(1) of the Kenyan Cybercrimes Act reflect the threshold test of harm articulated by the House of Lords in *Chambers v Director of Public Prosecutions (DPP)*.[70] In that case the lord chief justice held that 'a message which does not create fear or apprehension in those to whom it is communicated, or may reasonably be expected to see it, falls outside [the criminalized conduct] for the simple reason that the message lacks menace' (para. 30). To this extent, section 27(1) partially meets the best international practice standards. Still, despite the well-conceived elaboration of the harm caused by cyber-harassment in clauses (a) and (b), the prolix introductory sentence makes it difficult to ascertain the actions that are criminalised.

[67] *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 73.

[68] Constitution of Kenya, article 33(2): 'The right to freedom of expression does not extend to—(a) Propaganda for war; (b) Incitement to violence; (c) Hate speech; or (d) Advocacy of hatred that—(i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or (ii) Is based on any ground of discrimination specified or contemplated in Article 27(4).'

[69] *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 73.

[70] [2012] EWHC 2157 (Admin) (QB).

Other critical elements, such as what would constitute harassment or the repetitive nature of the offensive cyber-conduct, are not clarified in section 27(1) of Kenya's Cybercrimes Act.[71] The case law from the United Kingdom may offer useful guidance on this point. In *Jones v DPP,* the legal elements used to establish the offence of cyber-harassment were expounded in a concise way.[72] It was held that (i) the impugned conduct must form part of a sequence of connected acts, but each individual act forming part of the sequence need not be of sufficient gravity to be a crime in itself; (ii) the sequence of acts or course of conduct must involve incidents on at least two occasions and must not be two temporally distant incidents; and (iii) the fewer the incidents, the more serious its gravity should be to amount to harassment.

In this connection, two observations can be made regarding section 27(1) of the Kenyan Cybercrimes Act. First, it falls short of the required legal standards of certainty and should be amended to reflect this general principle of law.[73] Second, it conflates two distinct concepts – cyberstalking and cyberbullying – which should ideally be categorised as separate offences.[74]

It is noteworthy that neither the Budapest Convention on Cybercrime nor the Malabo Convention on Cyber Security have provisions for cyberstalking and cyberbullying. On one view, this may suggest that their constitutive conduct is not regarded as fit for criminal regulation. Indeed, comments on similar provisions in earlier legislative drafts of Kenya's Cybercrimes Act indicated that cybercrime or cybersecurity legislation was not an appropriate venue for addressing state failure to protect individuals from harassment, threats and other forms of intimidation.[75] This reflects the view that favours self-regulation of the Internet rather than regulation by way of prescriptive legislation.[76] It also fits with the principle of minimal criminalisation of cyber-conduct on the rationale that what is illegal offline is likewise illegal online.[77]

However, the central role that information and communication technology has come to play in social interactions and its prodigal capacity for facilitating criminal conduct may justify inclusion in national law of offences against cyberstalking and cyberbullying.[78] Indeed, some Commonwealth jurisdictions, such as Canada, New Zealand[79] and the United Kingdom,[80] have been persuaded to establish a regulatory framework

[71] Sugow, A., Zalo, M. and Rutenberg, I. (2021) 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression'. *Journal of Intellectual Property and Information Technology Law* 1(1).

[72] [2015] 1 WLR 833.

[73] *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33.

[74] *Wilson v R* [2012] VSCA 40.

[75] Article 19 (2018) *Kenya: Computer and Cybercrimes Bill 2017*.

[76] UK Government (2017) *A Safe and Secure Cyberspace – Making the UK the Safest Place in the World to Live and Work Online*.

[77] Criminal Code of Canada, section 243.

[78] Clough, J. (2014) 'A World of Difference'.

[79] Harmful Digital Communications Act 2015.

[80] Criminal Justice and Courts Act 2015, section 33; Malicious Communications Act 1988, section 1; Protection from Harassment Act 1997, sections 2A and 4A; Communications Act 2003, section 127.

to legally regulate online abusive behaviour. Their laws criminalise various forms of online harassment and bullying, including trolling, doxxing, identity theft and revenge pornography.[81] The guidance issued by the United Kingdom Crown Prosecution Service[82] relating to the effective prosecution of, among other crimes, cyberbullying and online harassment provides a reasoned basis for criminalising the conduct described in section 16(1) of the Kenyan Cybercrimes Act.

In addition, comparable cybercrime law from New Zealand can offer a suitable model for proposed amendments to section 27(1) of Kenya's Cybercrimes Act, as well as to other sectoral laws in Kenya. Section 6 of New Zealand's Harmful Digital Communications Act 2015 establishes 10 communications principles, including that digital communication should not be threatening, intimidating or menacing; incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual; be used to harass an individual; incite or encourage an individual to commit suicide; disclose sensitive personal facts about an individual; be grossly offensive to a reasonable person in the position of the affected individual; and be indecent or obscene.

These prohibited actions better illustrate some of the effects of the conduct criminalised in section 27(1) of the Kenyan Cybercrimes Act. Moreover, section 22(1) of the New Zealand Act defines the types of online and computer-related acts that may constitute the offence of causing harm by posting digital communication, and section 22(2) further specifies the relevant factors that should be considered by a court in 'determining whether a post would cause harm'.

Elements of the offence of cyber-harassment as specified in section 27(1) of the Kenyan Cybercrimes Act are inconsistent with the general principles of criminal law. The section does not specify the nature of the criminal intent as either fraudulent or malicious. Also, although it emphasises recurrence, it renders irrelevant the requirement of reasonable direct foreseeability of harm requirement. This may result in the criminalisation of possible erroneous actions that have no malicious intent.[83] In addition, the language used to describe the effects of the offence is vague and overbroad. It may be more constructive to require that the harm be not merely apprehended but also satisfy a higher and more definite threshold.

The comparable national cybercrime laws cited above adopt the legal standard of real or substantial risk. These are useful pointers for the reform of section 27 of Kenya's Cybercrimes Act. Also, as required under section 103 of the United Kingdom's Digital Economy Act 2017, it may be prudent to recommend that the cabinet secretary issue guidance to social media providers on actions that may be appropriate to take against online bullying, intimidation or humiliation.

[81] Strickland, P. and Dent, J. (2017) 'Online Harassment and Cyber Bullying'. Briefing Paper 07967. London: House of Commons Library.

[82] UK Crown Prosecution Service (2018) *Legal Guidance on Stalking and Harassment*.

[83] Herring, J. (2014) *Criminal Law: Text, Cases, Materials*. Oxford: Oxford University Press.

Besides an indeterminate definition of cyber-harassment in section 27(1) of the Kenyan Cybercrimes Act, the penalty for cyberstalking and cyberbullying is also questionable. Section 27(2) of the Act prescribes that, on conviction for this offence, the guilty party is liable to 'a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.'[84] This sanction is excessive and unjustified. It must be borne in mind that the acts that this offence encompasses frequently occur in the context of social relations and are a product of its breakdown.[85] Accordingly, draconian law and punitive sanctions may not be an appropriate response to this social issue.[86]

Consider the case of *A M v Premier Academy*, which was decided before the enactment of the Kenyan Cybercrimes Act.[87] The brief facts of the case are that a child was suspended from school on account of bullying other students by means of a social media network. Had section 27 of Kenya's Cybercrimes Act been in force, that child may have risked far more than just mere suspension from school: a steep fine and significant prison time. Another real risked posed by the provisions of section 27 is its potential abuse by governmental authorities to target activists and investigative journalists who routinely criticise public officials and expose their unlawful and risqué transgressions. This risk has already materialised, as illustrated by the case of *Republic v Robert Alai*.[88] In this case, a blogger who criticised the president on his Facebook page challenged the constitutionality of the decision to charge him.

4.9 Ancillary criminal law provisions

Section 46 of the Kenyan Cybercrimes Act outlines an ancillary criminal law provision to supplement the existing law by adding an enhanced penal regime if an offence is committed by cyber means. It stipulates that 'A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.' The effect of section 46 of the Act is to impose on an already established sentencing regime a mandatory requirement that judicial officers should add significant penalties for the mere reason that an offence was committed through the use of a computer system. This provision is inappropriate for at least two reasons.

First, it results in the duplication of legislative effort because the Kenyan Cybercrimes Act criminalises a broad range of offences that effectively encompass conduct for which section 46 of the Act seeks to impose an additional penalty. These offences can be categorised as including (i) offences against the confidentiality, integrity and availability of

[84] The amount of Ksh 10 million is approximately US$82,045.

[85] BAKE (2018) *State of the Internet in Kenya 2017.*

[86] Brenner, S. (2007) 'Cybercrime: Re-thinking Crime Control Strategies', in Y. Jewkes (ed.) *Crime Online.* Cullompton: Willan Publishing.

[87] [2017] eKLR.

[88] [2017] eKLR.

computer data and systems; (ii) computer-related offences; (iii) content-related offences; (iv) offences related to the breach of copyright or related rights; and (v) privacy and data protection offences.

Additionally, most of the offences outlined in the Act attract substantial fines, ranging between not more than Ksh 5 million[89] and Ksh 20 million,[90] and prison terms ranging between sentences not exceeding three years and ten years. There is also the possibility of getting a fine and a prison sentence. Moreover, the majority of serious offences that may be committed by cyber means are already criminalised in the Penal Code and in specialist statutes. When considered cumulatively, it is clear that section 46 of Kenya's Cybercrimes Act is not consistent with the legal principle of minimal criminalisation, and it is also unclear what public policy aims its draconian approach would serve.

Second, section 46 of Kenya's Cybercrimes Act fails to satisfy the imperative of legal certainty.[91] Its scope is both imprecise and overbroad because it ambiguously refers to offences under any law committed through the use of a computer system. Yet it does not specify the unlawful act, nor make clear the manner in which the use of a computer system will expose one to criminal liability. This indefinite wording invariably makes the targeted criminal conduct indeterminate, and this means the section runs the added difficulty of being open to abuse.

5. Conclusion

This article has demonstrated that, while the Kenyan Cybercrimes Act is a creditable legislative step towards the end of tackling cybercrimes in Kenya, some of its provisions raise serious concerns that need to be addressed by way of amendment. Although the notable merits of the Act are no less important, the overriding interest of providing meaningful guideposts on points for reform dictate that its shortfalls be restated first, followed by the proposed corrective steps that must be taken to ensure that the Act is both effective and constitutionally compliant. Accordingly, by way of summary of the points raised and concluding observations, below is a non-exhaustive scorecard of the Kenyan Cybercrimes Act.

With reference to certain provisions discussed above,[92] the Kenyan Cybercrimes Act adopts a punitive and slipshod approach to drafting criminal offences. It has embraced such an excess of zeal in criminalising actions that it overlooks the duplication of offences.[93] With a few notable exceptions, the Act gives insufficient attention to the imperative of legal certainty by failing to specify the key elements of specific intent and the degree of harm.[94] In addition, it ardently adopts exacting sentences and onerous fines

[89] Approximately US$41,022.

[90] Approximately US$164,090.

[91] *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33.

[92] See Sections 4.3 and 4.4 of this article.

[93] See sections 6, 7 and 10.

[94] See Section 4 of this article.

but shows little attention to the proportionality of the sentence *vis-à-vis* the gravity of the crime or the public policy objects that are to be served by the respective sanctions. Most problematic of all, Kenya's Cybercrimes Act insidiously expands the scope of ever-greater governmental restriction on fundamental human rights, particularly when its provisions are read together with the Security Laws (Amendment) Act 2014.[95]

Despite its shortcomings, some consolation may be found in the fact that there is still an opportunity to rectify by statutory amendment the legitimation of these elements of bad law in the Kenyan Cybercrimes Act. Better still, there are specific ways by means of which this important task may be accomplished. First, there is a need for more inclusive stakeholder engagement with the Kenyan Cybercrimes Act. Thus far, public participation in the legislative and subsequent implementation processes has been modest and superficial. There has also been a marked absence of youth participation in these processes, whereas this is the demographic group that the provisions of the Act are most likely to affect.

Second, there is an urgent need to reconsider and redraft the criminal offences section so as to remove some duplicative provisions, to clearly delimit the scope of the offences and to better specify the objective and subjective elements of crime. As discussed in this article in relation to specific offences, a number of provisions overlap with or are essentially the same as others.[96] With more judicious drafting, the number of offences can be reduced, with some duplicative offences being removed altogether.

Third, the needlessly punitive regime of sentences in Kenya's Cybercrimes Act needs to be abandoned and replaced with a more context-sensitive and proportionate approach. Towards this end, it may be useful for lawmakers to have regard to the Sentencing Guidelines adopted by the Judiciary in 2015,[97] as well as to case law from the Supreme Court of Kenya.[98] Also, most of the sanctions in the Kenyan Cybercrimes Act do not draw a distinction between serious and less serious types of harm. This makes it possible for an individual guilty of cyber-conduct causing a small degree of harm to receive punishment similar to that facing another whose action results in more serious damage. Nor do the sanctions in the Act specify that only offences with criminal or dishonest or fraudulent intent attract the heavy penalties. For these, among other, reasons, the sanctions regime in the Kenyan Cybercrimes Act needs to be reformed systematically.

[95] *Law Society of Kenya v Attorney General and Another; National Commission for Human Rights and Another (Interested Parties)* [2020] eKLR; *Okiya Omtatah Okoiti and 2 Others v Cabinet Secretary, Ministry of Health and 2 Others; Kenya National Commission on Human Rights (Interested Party)* [2020] eKLR.

[96] See Section 4.7 of this article.

[97] Judicial Service Act, Sentencing Guidelines, 2016 Gazette Notice No. 2970 of 29 April 2016.

[98] *Francis Karioko Muruatetu and Another v Republic* [2017] eKLR.

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Funding Crime Online: Cybercrime and its Links to Organised Crime in the Caribbean

Sophie Brain[1] and Olajide Oyadeyi[2]

Abstract

The Caribbean region has seen an explosion in digital transformation, with one of the fastest growing internet populations worldwide. The accompanying growth in cyber technology has allowed for new regional and social advancements. However, the Caribbean has also become an attractive target for cybercrime due to increased economic success, a growth in online presence, combined with low levels of cyber resilience. Organised crime groups have been able to exploit these vulnerabilities by taking advantage of the internet and exploring new ways of making money online, as well as using the internet for other illicit activities such as money laundering and funding terrorism. The Caribbean remains acutely unprepared to deal with cyberattacks and the COVID-19 pandemic highlighted several instances where these weaknesses were exposed, allowing for criminal groups to make millions of dollars.

This paper therefore aims to analyse the relationship between organised crime groups and cybercrime in the Caribbean and explores the methods used by these groups to fund their activities. The concept of 'software-as-a-service' is highlighted as an enabling factor in the underground economy used by organised crime groups in the Caribbean to help facilitate cybercrime. Ransomware is discussed as one of the top security concerns in the region, often used by organised crime groups to demand payment from organisations with insufficient cyber defences. Phishing is also emphasised as a common technique used by organised crime seeking to steal user banking data, gain access to accounts and steal from victims. Digital currencies such as Bitcoin, Ethereum and Central Bank Digital Currencies, as well as the dark web, are discussed as main facilitators used to move criminal proceeds in the Caribbean. The paper also discusses what

[1] Research Officer, Commonwealth Secretariat. Email: sophie.brain@hotmail.com

[2] Economic Research Officer, Commonwealth Secretariat. Email: jide.oyadeyi@gmail.com / o.oyadeyi@commonwealth.int

Commonwealth Caribbean countries have done so far to combat these issues through their national cybersecurity strategies, including Jamaica's National Cybersecurity Strategy and Belize's National Cybersecurity Strategy – Towards A Secure Cyberspace 2020–2023. The activities of regional groups such as the Caribbean Community and Common Market (CARICOM) Cyber Security and Cybercrime Action Plan are highlighted. Examples of successful interventions to undermine the use of cybercrime by organised crime groups in the world's leading cybersecurity authorities are also explored.

Introduction

Cybercrime has been common since the advent of the internet. The cost of cybercrime in recent times has, however, become more pronounced. According to Cybersecurity Ventures (2022), the world was due to lose over US$7 trillion to cybercrime in 2022, after losing more than US$6 trillion in 2021. If this figure was measured as a country, cybercrime would be the third-largest economy after the US and China. However, cybercrime cannot be discussed in isolation. This is because cybercrime is linked to the level of information and communication technology (ICT) in a country, and ICT has been used as a tool to integrate different systems across sectors or countries. For instance, many entities and organisations use ICT for their basic tasks. This has made it possible for many cybercriminals to target and defraud institutions and individuals. According to Verizon's (2022) *Data Breach Report*, 82 per cent of breaches involve a human element. That is, whether by phishing, the use of stolen cards, misuse or an error, human beings play a dominant role in cybercrime today. The globalisation of markets and the interconnectedness of states, combined with reliance on ICT, calls for both developed and developing states to put into place measures to address cybercrime.

This is especially true in the Caribbean, as the region's internet penetration since the turn of the twenty-first century has been on the rise. Internet users averaged 67.4 per cent of the total population in the region in 2020 compared to 52.4 per cent worldwide (WDI 2022a). This gives more credence to the notion that increased internet usage across the Caribbean has led to the proliferation of cybercriminal activities, making the region more vulnerable to cybersecurity attacks. Despite increased awareness and attention directed towards this problem, cybercrime remains a complex issue. In 2016 for example, Jamaica lost in excess of US$77 million to cybercrime alone (Wilson-Harris, 2019). These losses have adverse effects on business revenues, the cost of operations, individuals and the government in terms of its ability to provide welfare packages across the Caribbean. Furthermore, the introduction of cryptocurrencies, a platform for trading virtual currencies, has brought about renewed vigour in regulating online activities.

Analysing the Caribbean region in the context of the global discourse on cybersecurity and cybercriminal activities is particularly important. This is due to the compounding effect cybercriminal activities may have on the countries' economies given their small size, inherent small country characteristics and the specific vulnerabilities that they face. In comparison to the US, where a cyberattack may not significantly affect the entire economy, weak infrastructure in the Caribbean – as well as the centrality of information within governments – makes the region more vulnerable to cybersecurity breaches and cybercriminal activities, which may cause a national crisis that could affect the entire macroeconomy. Moreover, the discourse on cybercriminal activities and cybersecurity breaches is becoming a developmental issue. This is because, in the event of a breach, the affected state would witness rising economic costs. These costs would be more amplified in a small and developing country context (Wint 2003; Moore 2017). Wint (2003) opined that cybercrime tends to affect small countries more than larger countries due to the larger countries' ability to cushion the effect better at the national level compared to a smaller country. By implication, a cyberattack or breach on government infrastructure and private sector organisations would affect a small Caribbean country to a larger extent (Moore 2017).

Furthermore, the ease of doing business is of top concern to several small Caribbean states as they continue to rebuild their economies following the COVID-19 pandemic, which had a significant impact on businesses in the region (Hamilton-Davis 2023). This cannot be achieved without focusing on cybersecurity as cybercrime has implications for companies, causing increased costs as organisations incur outlays such as cybersecurity technology or expertise and insurance premiums to protect their businesses. In addition to this, high levels of cybercrime cause reputational damage as customers, and even suppliers, may feel less secure leaving their sensitive information in the hands of a company whose information technology (IT) infrastructure has been broken into, which could lead to lost revenue. Given the high economic cost of infrastructural protection from cybercrime, coupled with Caribbean small states' limited financial resources, this has caused the region to be particularly vulnerable to escalating cybercriminal activity.

It is because of these increased vulnerabilities faced by Caribbean states that this study aims at adding to the literature on cybercrime and its links to organised crime in Commonwealth Caribbean countries. The objectives of this paper are therefore to conceptualise cybercrime in the region and identify the types of crimes being carried out by organised crime groups and their impacts on Commonwealth Caribbean countries. Furthermore, the paper aims to identify ways through which cybercrime can be reduced, offering guidance to Commonwealth Caribbean countries on how this can be done.

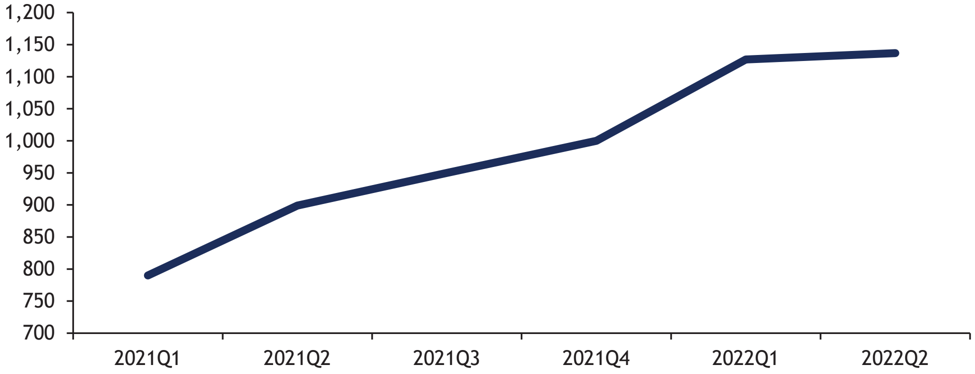
The rest of the paper is organised as follows. The next section introduces some stylised facts about global cyberattacks and links between ICT and cybercrime in the Commonwealth Caribbean countries. The section that follows explores the scope of organised crime in the Caribbean. There is then a section that discusses how organised crime groups are using cybercrime and identifies the different types of cybercrime that occur in the region. The next section discusses existing legislation and strategies used in combating cybercrime among Commonwealth Caribbean countries, while the final section identifies means by which cybersecurity can be improved and offers learning experiences from leading cybersecurity authorities.

Stylised facts

Stylised facts on cybercriminal activities across the globe

In recent times, the world has been affected by increased cyberattacks, as evidenced in Figure 1. Cybercriminal attacks per organisation grew from 899 attacks in Q2 2021 to 1,136 attacks in Q2 2022, an increase of 32 per cent year-on-year. According to Check Point Research (2022b), this has been the highest rate of weekly increase in cybercriminal activities since the introduction of the internet, leading to questions surrounding the safety of individuals, corporate organisations and governments from cybercriminals.

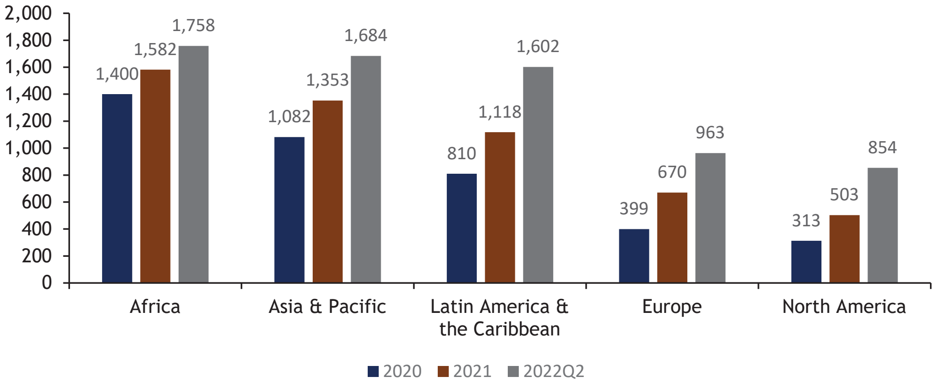
Figure 1. Global weekly cyberattacks



Source: Check Point Research 2022a

Figure 2 shows that by region, Africa has been most affected by cybercriminal activities, followed by Asia, and Latin America and the Caribbean (Check Point Research 2022a; 2022b). Looking through the data in more depth, it can be seen that between 2021 and Q2 2022 the Latin American and Caribbean region witnessed the largest increase in average weekly cybercriminal attacks per organisation (484) when compared to other regions. This therefore emphasises the importance of focusing on cybercrime in Caribbean Commonwealth countries, as cybercrimes have increased more there than in other regions.

Figure 2. Weekly cyberattacks by region



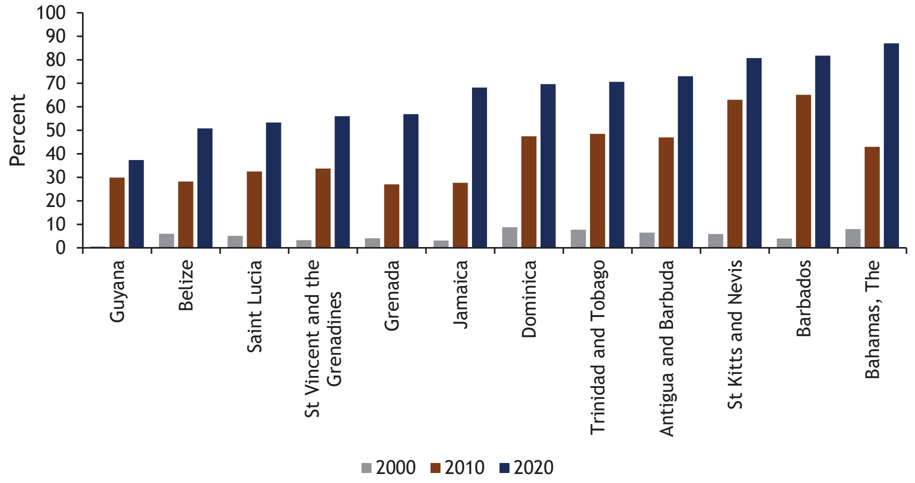
Source: Check Point Research 2022a; 2022b

Stylised facts on ICT performance and links to Cybercrime in Commonwealth Caribbean countries

Due to the proliferation of internet usage between 2000 and 2020, cybercriminals have used the opportunity to advance their illegal activities, while advances in ICT may provide a useful opportunity for the growth of illegal activities if not properly regulated. The Caribbean region has made significant strides in ICT development, especially between 2010 and 2020 – as demonstrated in Figure 3. In the year 2000, the average proportion of internet users in the Commonwealth Caribbean region stood at 5 per cent of the population, with Dominica having the highest internet usage at 9 per cent while Guyana had the least internet usage at 0.60 per cent of the population. Between 2000 and 2010, the average internet usage increased to 41 per cent, a rise of 683 per cent from the year 2000.

Between 2010 and 2020, the average number of internet users as a percentage of the Commonwealth population in the Caribbean grew by 59 per cent, from 41 per cent in 2010 to 65 per cent in 2020. Due to the rapid increase in internet use, the growth in internet penetration between 2000 and 2020 stood at 1,147.7 per cent. This growth in internet users may be ascribed primarily to a rise in internet access through mobile devices, reduced internet costs and the rise in e-commerce. This has implications for cybercriminal activities, as with faster and cheaper internet connectivity, cybercriminals have more opportunities to engage in online crime as they are able to increase their reach. These increased opportunities, paired with limited cybercrime legislation, make the region a prime target for cybercriminals.

Figure 3. Users of the internet (percentage of population)

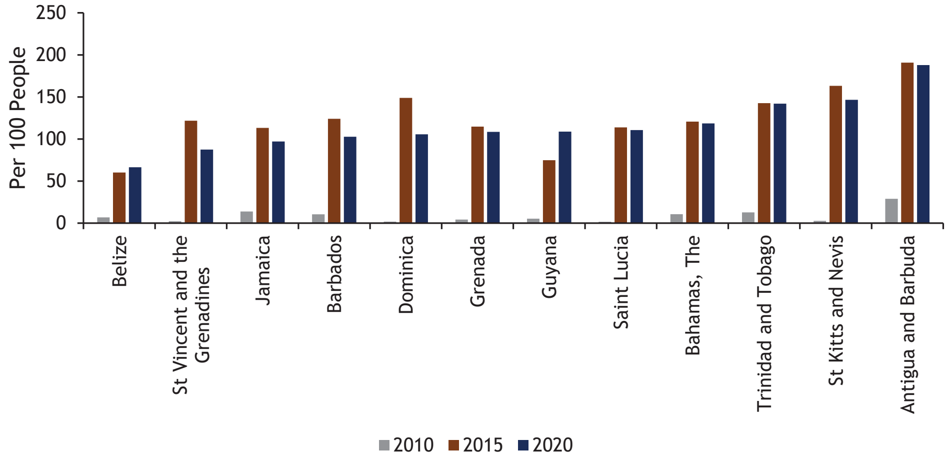


Source: World Development Indicator (WDI) 2022a

Figure 4 depicts the trend of mobile cellular subscriptions across Commonwealth countries within the Caribbean region. In 2010, the average mobile cellular subscriptions in the Caribbean region stood at 8.43 people per 100 people. At this point, Antigua and Barbuda had the highest number of mobile cellular subscriptions at 29 people per 100, while Saint Lucia had the least at 1.60 people per 100. In 2015, the average mobile cellular subscription in the Caribbean region grew by 1,372 per cent, from 8.43 people per 100 to 124.08 people per 100, given that certain individuals at that stage may have had more than one mobile phone subscription.

In 2020, the growth in the average mobile cellular subscriptions fell by 7.18 per cent, from 124.08 people per 100 in 2015 to 115.2 people per 100. This could be due to users consolidating their cellular subscriptions as costs increased. Like previous years, Antigua and Barbuda had the highest number of mobile cellular subscriptions at 187.9 people per 100, while Belize had the least number of mobile cellular subscriptions at 66.39 people per 100. From these figures, it is clear that remote connectivity is high across Commonwealth countries in the Caribbean as the average for middle-income countries is 108 per 100 and 122 per 100 for high-income countries (WDI 2022b). The reliance on mobile phones to access the internet in the Commonwealth Caribbean also has implications for cybercrime, as mobile devices tend not to have firewalls, antivirus software, encryption and other defensive mechanisms that computers do, making them more vulnerable to threats. Examples of this occurring in Caribbean Commonwealth countries will be explained in detail later in the paper.

Figure 4. Mobile cellular subscriptions (per 100 people)



Source: WDI 2022a

Table 1 shows information on secure internet servers in the Caribbean Commonwealth countries between 2010 and 2020. Data on other regions, as well as selected Commonwealth countries, were also selected for comparison. In 2010, Antigua and Barbuda had the highest number of secure internet servers at 681.6 people per1 million, while Guyana had the least number of secure internet servers at 1.3 people per 1 million. In 2020, while Guyana continued its trajectory as the country with the least secure internet servers at 61 people per 1 million, Belize significantly improved its numbers of secure internet servers and became the most secure Commonwealth country in terms of internet servers within the Caribbean.

In comparison to other regions such as the Euro Area, it is evident that Belize and Dominica performed admirably well in 2020 (see Table 2). Furthermore, their performance far outstrips the Latin America and the Caribbean region, as well as other selected advanced Commonwealth countries such as Australia, Canada and the United Kingdom. The adoption of a cybersecurity strategy in Belize may have helped improve its secure internet connections, while the Government of Dominica has made significant strides to upgrade its resilience against potential cybercrimes by partnering with international organisations to achieve its goal. These among other policies may have helped these two countries to significantly improve their secure internet connections compared to others within the region.

Although, St Kitts and Nevis is well above the Latin America and Caribbean average, with a secure internet connection of 6,223 per 1 million people, it is still far from reaching the levels of other advanced nations. On the other hand, the rest of the Commonwealth Caribbean countries are well below the Latin America and Caribbean average, as well as the World and Euro Area averages. This implies that more work needs to be done to improve the number of secure internet connections across Antigua and Barbuda, The Bahamas, Barbados, Grenada, Guyana, Jamaica, Saint Lucia, St Vincent and the Grenadines, and Trinidad and Tobago, as this could have implications for these countries' cybersecurity.

Table 1. Secure internet servers (per 1 million people) across Commonwealth Caribbean countries

	2010	2015	2020
Antigua and Barbuda	681.6	694.7	1,245.8
Bahamas, The	366.3	1,002.1	1,261.3
Barbados	187.9	574.8	1,037.0
Belize	214.0	1,141.5	131,343.7
Dominica	42.3	266.9	46,922.5
Grenada	94.1	219.0	577.7
Guyana	1.3	27.4	61.0
Jamaica	24.2	121.4	160.4
St Kitts and Nevis	550.9	742.1	6,222.7
Saint Lucia	46.0	139.6	375.8
St Vincent and the Grenadines	18.5	119.1	126.2
Trinidad and Tobago	44.4	269.3	340.1

Source: WDI 2022a

Table 2. Secure internet servers (per 1 million people) across selected countries and regions

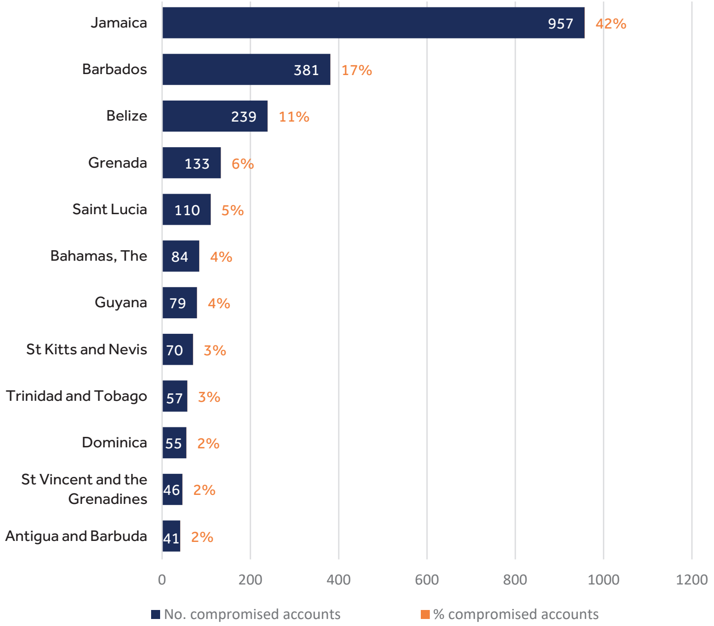
	2010	2015	2020
Euro Area	544.0	2,493.8	51,693.2
Latin America and the Caribbean	21.3	106.4	1,963.7
World	187.3	572.7	11,499.7
Australia	1,402.8	4,574.1	39,794.4
Canada	1,282.7	3,386.9	39,849.7
United Kingdom	1,315.4	4,386.3	36,379.7

Source: WDI 2022a

Due to the low levels of secure internet services across certain Commonwealth countries in the Caribbean, cybercriminals have taken advantage by developing ways of compromising emails, accounts and other online activities. Research carried out by G5 Cybersecurity (2021), as presented in Figure 5, shows that from a total of 2,252 compromised accounts across the Commonwealth countries in the Caribbean, Jamaica had the highest number of compromised accounts in 2021. This was closely followed by Barbados (17%) and Belize (11%). These figures support the relationship between the number of secure internet servers and compromised accounts as the number of secure internet servers is very low across these countries, as displayed in Table 1, since Jamaica and Barbados had 160 and 1,037 secure internet servers per 1 million people in 2020, which was relatively low when compared to advanced Commonwealth countries. However, Belize has high levels of secure internet servers, suggesting the relationship may not be so direct.

On the other hand, Antigua and Barbuda (41), St Vincent and the Grenadines (46), and Dominica (55) had the least number of compromised accounts within the Caribbean. The link between low levels of compromised accounts in this case can clearly be seen, as Dominica has relatively high numbers of secured internet servers when compared to the rest of the region. Caribbean Commonwealth countries need to be mindful when it comes to ensuring that they adequately inform individuals and businesses on securing their accounts, as this could have large economic consequences.

Figure 5. Number and percentage of compromised accounts across Commonwealth Caribbean countries in 2021



Source: G5 Cybersecurity 2021

Increased levels of internet usage, high numbers of mobile cellular subscriptions, and a lack of secure internet servers in certain Caribbean Commonwealth countries provide some insights into why cybercrime is taking place in the region and why it is likely to grow moving forward. Furthermore, the COVID-19 pandemic has acted as a great accelerator of digital transformation, with technology being at the forefront of countries' responses to the crisis. Although cybercrime was increasing and transforming before the pandemic, with a record number of people staying in their homes and relying even more on the internet for daily activities including work, education and leisure than usual, the ways for cybercriminals seeking to exploit emerging opportunities and vulnerabilities multiplied during this time (Europol 2020).

The pandemic therefore exposed the fragility of e-government services, online consumer services and education, and exacerbated the many inequalities in the system in the Commonwealth Caribbean. Cybercriminals took advantage of the crisis, since most jobs shifted operations online, and they were able to use a combination of online ransomware, phishing and other forms of cybercrime such as cryptocurrency fraud to swindle organisations, investors and individuals, further worsening this crisis. The following sections provide a more in-depth look at organised crime groups in the Caribbean and how they have used cybercrime to carry out their activities both before, during and after the COVID-19 pandemic.

Scope of organised crime in the Caribbean

Organised crime groups, which are defined in this article as groups that have as their purpose, or one of their purposes, the carrying out of criminal activities, and consist of three or more people who agree to act together to further that purpose, operate throughout the Commonwealth Caribbean. This is given its appealing geography, which allows for criminality to flourish. The Caribbean's border proximity to South America makes it both a destination and a transhipment zone for the trafficking of illicit drugs and arms to Florida, the East and Gulf Coasts of the United States (US), and to points throughout Europe and Africa (White House 2022). Large amounts of cocaine, marijuana and other drugs transit through Jamaica, Trinidad and Tobago, The Bahamas, and the Eastern Caribbean.

The influence of South America on the region has meant that foreign criminal organisations, most notably from Colombia and Mexico, feature in these countries' underworlds (Global Initiative 2020a). There is also evidence of the Italian mafia operating in The Bahamas, using the country as a trans-shipment point for cocaine trafficking. Furthermore, the ongoing political instability of the Government of Venezuela continues to generate new opportunities for organised criminal activities (White House 2022).

Street gangs are also active in much of the Caribbean region, with Jamaica reporting more than 260 gangs with nearly 4,000 members and Trinidad and Tobago identifying 95 gangs with more than 1,200 members (Katz 2015). These gangs are linked to the region's high homicide rates, with organised crime groups able to exert social control and co-opt the state in a variety of ways (InSight Crime 2018). In countries like Jamaica, for example, government sectors have established political alliances with local gangs to compensate for the state's abandonment of certain communities. Trinidad and Tobago's gangs also perform key social functions (ibid).

Given that drug trafficking is the main source of 'dirty money' in the region, both tax evasion and fraud take place as a knock-on effect of the funds from drug sales. Illicit flows are often legitimised through legal businesses such as real estate, private member clubs and banks. In addition to this, because many Caribbean countries implement liberal tax regimes while also permitting the formation of offshore companies to attract foreign investment, this allows for both shell companies to set up and tax avoidance schemes to take place. These shell companies can be used as money laundering systems to disguise the origin of illegal funds and help criminals to avoid anti-money laundering measures (Comply Advantage 2022). Ponzi and pyramid schemes also operate across the region, sometimes facilitated by army personnel and high-ranking government officials, increasing their reach (Global Initiative 2020b).

The prevalence of organised crime groups in the region has also allowed for criminal activity that goes beyond drug smuggling and arms trafficking. For example, Trinidad and Tobago is a source, transit and destination country for human trafficking. Women and girls from Venezuela, the Dominican Republic, Guyana and Colombia are vulnerable to sex trafficking in Trinidad and Tobago's brothels and clubs, while economic migrants from the Caribbean and Asia are vulnerable to domestic servitude and forced labour in the retail sector (Global Initiative 2020b).

Both fauna and flora crimes take place in the Caribbean region, with deforestation being a main issue. This is especially the case for Guyana, which is a source country for precious woods that are mainly shipped to China. Some Caribbean Commonwealth nations are also source and transit countries for the illegal trafficking of some of the world's most threatened species of fauna, including parrots, macaws, parakeets, songbirds, reptiles, arthropods and jaguars (Global Initiative 2020c). This trade in wildlife has increased significantly since the economic crisis in Venezuela, with an expanding number of traffickers identified.

The internet is a major enabler for organised crime groups' previously described activities in the Caribbean. There has been evidence that traditional organised crime groups have engaged in cybercrime and have been able to use the internet as a communication, research, logistics, marketing, recruitment, distribution and monetarisation tool (UNODC 2013; UNODC 2012). For example, organised crime groups use the dark web – encrypted online content that is not indexed by conventional search engines – for the illicit online trade in drugs, weapons, stolen goods, stolen personal and payment card data, forged identity documents, and child abuse material (George, 2018). Furthermore, hacking – which can be defined as the unauthorised use of, or access into, computers or network resources which exploits identified security vulnerabilities in networks – individuals, small and medium-sized enterprises (SMEs), and large organisations is a low-cost, low-risk proposition for criminal groups compared to making money from more traditional forms of crime (Home Office 2013 & National Cyber Security Centre 2017).

These organised crime groups operate either partially, predominately or solely online (UNODC 2019). However, there are cases of networks that have been formed and/or operate exclusively and/or predominantly online. These changes have allowed for increased cybercrime activity to take place in the region.

How are organised crime groups using cybercrime?

As we better understand the nature of organised crime in the Caribbean, we can start to look at what implications this has for cybercrime. Cybercrime can be divided into two main areas: cyber-enabled crimes, which are traditional crimes that can be increased in scale by using computers; and cyber-dependent crimes, which can only be committed through the use of online devices.

Cyber-enabled crimes: phishing, skimming and the use of social media

As we have already established the scope of organised crime activities in the Caribbean, we will first analyse cyber-enabled crimes across the region. Cyber-enabled crimes in the Caribbean have proliferated with increased internet usage, making individuals more vulnerable to nefarious activity. Phishing, which is when a criminal attempts to lure users to counterfeit websites in hopes of acquiring private information such as usernames or passwords, has become a common occurrence across the region. We have seen evidence of this in Dominica, where in 2021 spam emails with the subject 'Important Information Regarding your NBD Account(s)' were sent to individuals masquerading as being from the National Bank of Dominica Ltd, with the goal to steal the personal information of the individuals (National Bank of Dominica 2021). Furthermore, the National Commercial Bank (NCB) of Jamaica was also hit by a phishing and smishing (a phishing cybersecurity attack carried out over mobile text messaging) scheme, where customers were asked to click on links and give up personal information. The scammers would then carry out a follow-up phone call disguised as NCB employees with requests for the token code that customers are required to input to access certain services. The scammers would then use the code to add themselves as beneficiaries on the customers' accounts and to then transfer funds (Mckenzie 2022). Skimming, which is when thieves capture credit card information from a cardholder without their knowledge, is also taking place in Trinidad and Tobago. Skimmers have established a foothold in the country, with networks in operation – usually comprising foreigners, and more specifically Venezuelans – who have access to special equipment (Superville 2021).

Online romance or social networking/dating website frauds are also common across the Commonwealth Caribbean. This usually occurs when individuals are contacted via social networking or dating sites and persuaded to part with personal information or money following a lengthy online 'relationship' (Home Office 2013). There has been evidence of this in Guyana, where the Guyana Police Force alerted citizens concerning a scam involving persons suspected of pretending to be of Nigerian nationality. This scam would usually work by the individual sending a Facebook friend request to the victim and subsequently requesting their phone number for communication via WhatsApp. As time progresses, the criminal expresses an amorous interest in the intended victim and indicates that he/she would be sending some gifts for her/him, including jewellery (Guyana Standard 2020). The victim must then pay for these gifts to be released from customs; however, the gifts never materialise (ibid). There have also been reports of romance scams in Trinidad and Tobago, with around US$300,000 lost to these scams between 2020 to 2021 (*Trinidad and Tobago Guardian* 2021).

Across the Caribbean, but specifically in Barbados and Trinidad and Tobago, there have been instances where social media is used to expand organised crime groups' operations. In Trinidad and Tobago, social media has been used in several cases to recruit victims into human trafficking, as criminals move from social media sites to chatrooms to lure individuals (Douglas 2022). Authorities in Barbados have also noted an increase in social media being used to recruit victims into human trafficking (IOM 2015). In addition to this, criminal drug networks are abusing social media to expand their reach, create new markets and target new clientele. This has been exemplified in Belize, where gang members posted video on social media showing several unlicensed and prohibited firearms; this later went viral, helping to expand the group's reach and reputation (*Breaking Belize News* 2022).

Cyber-dependent crimes: hacking, ransomware, and Central Bank Digital Currencies

Cyber-dependent crimes are primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks, such as data gathered by hacking that can then be used to commit fraud. Across the Caribbean, we have seen a range of examples where hacking has taken place. In some instances, hacking takes place to deface government websites and promote specific ideologies or messaging. This was the case for The Bahamas in 2015, which saw its Ministry of Tourism websites hacked by members of a Tunisian Islamist activist group called the 'Fallaga Team' who were attempting to promote Islamist ideology (Eleutheran News 2015). In the same year, St Vincent and the Grenadines also had its official government website hacked by the radical Islamist group the Islamic State as it posted a photograph of a man on the back of a pickup truck firing a machine gun and the headline 'Hacked by Moroccanwolf – Islamic State' (CARICOM 2015). In 2019, Trinidad and Tobago government websites, including those belonging to the Ministry of National Security, the Immigration Division and the Attorney General's Office, were also hacked (Popplewell 2019). The hacker, known as 'VandaTheGod', is Brazilian based and known for posting political messages. In this instance, he called the Government of Trinidad and Tobago corrupt and tried to make citizens hold the government accountable for its actions.

In some cases, hacking occurs and is then followed by a ransomware attack. These ransomwares attacks arise when hackers freeze access by victims to their data, either by locking the system's screen or by locking the users' files until a ransom is paid. This was the case in both Jamaica and Trinidad and Tobago, when the Massy Stores and Massy Distribution companies were hacked in 2022 and it was confirmed they were then victims of a ransomware attack. Five months after the attack, 17 gigabytes of data were dumped on the internet by cybercriminal group, Hive Ransomware, including personal information such as the names, addresses, taxpayer registration numbers, and signatures of Massy employees and contractors (Barrett 2022). The result of this data-dump was customers, employees, suppliers and the wider financial sector were then easy targets for hackers and fraudsters engaged in identity theft (ibid). In 2020, Ansa McAl, the Caribbean's biggest conglomerate, was also held hostage by a ransomware attack by criminal cybergang REvil in both Trinidad and Tobago and Barbados (Bridglal 2020). The criminal cybergang then released 12.9 gigabytes of Ansa's data, allegedly because the company refused to pay a ransom (ibid).

Both the hacking of Massy and Ansa McAl highlight how cybercrime is developing in the Caribbean region. The groups involved in the attack are ransomware-as-a-service (RaaS) or software-as-a-service (SaaS) operations, which is a business model between ransomware operators and affiliates in which the affiliates pay to launch ransomware attacks developed by operators. This means that individuals or groups both inside and outside the Caribbean who want to carry out cyberattacks no longer need to develop their own cyber skills, as these can be outsourced. Individuals or groups wanting to cause damage can now find hackers through the dark web and vice versa. These types of ransomware attacks could also be a sign that state-sponsored operations are becoming more frequent in the region, as nation-states seek to exploit Caribbean countries' vulnerabilities or gather intelligence.

Cryptocurrencies, which are a digital means of exchange that use cryptography for security, are increasingly used to make purchases across the world (Kurmi 2022). However, cryptocurrencies such as Bitcoin and Ethereum, are also used to move criminal proceeds. An example is the Mexican cartels, including the Jalisco New Generation Cartel and the Sinaloa Cartel, which use Bitcoin to launder money. These gangs typically split their illicit cash into small amounts and deposit them in various bank accounts, a technique known as 'smurfing' (Oré 2020). They then use those accounts to buy a series of small amounts of Bitcoin online, obscuring the origin of the money and allowing them to pay associates elsewhere in the world (ibid). With countries in the Caribbean being relatively open to cryptocurrencies, such as St Kitts and Nevis implementing legislation to make crypto transactions easier, there are risks that these loopholes could be exploited by organised crime groups to launder money and carry out illegal goods transactions across the region.

The rise of cryptocurrencies in the region will also facilitate the use of the dark web, as transactions typically take place using digital currencies (George 2018). In the past, we have seen cartels exploring the dark web to locate buyers for large-scale cocaine shipments, while Central American gangs have used these sites to advertise their willingness to help with cross-border trafficking (ibid). Given the different types of criminal activity taking place in the region, there is a high chance the dark web is being used to facilitate organised criminal activities.

Caribbean central banks have also been active in exploring Central Bank Digital Currencies (CBDCs), with three launched so far in the region. These CBDCs are the digital form of a country's fiat currency and are similar to cryptocurrencies as they are digital tokens (BIS 2021). However, these CBDCs are issued by central banks and are not privately owned, in contrast to cryptocurrency. Nonetheless, there are still risks when it comes to cybersecurity and financial crime as although the central banks issue the currencies, they use third party infrastructure and software – which could potentially open the door to fraud and illicit payments. This will drive cybercriminals to seek ways to steal and abuse monetary systems as these CBDCs are further implemented across the region.

The impact of COVID-19 on cybercrime activities

The COVID-19 crisis accelerated changes that were already underway in the criminal economy, especially online. Industry data from all over the world showed meteoric rises in internet usage, 50 to 60 per cent higher, from 2020 to 2021 (Reitano and Shaw, 2021). Without increased cyber surveillance, criminals used the COVID-19 crisis to bombard individuals and businesses with misinformation, distribute malware, and conduct phishing attacks and scams (ibid).

There is clear evidence that the COVID-19 pandemic had implications for cybercrime activities in the Caribbean. The prevalence of a social media scam that involved the impersonation of government ministers in Grenada was a prime example of this issue. The scam consisted of offering COVID-19 assistance packages, ranging from US$30,000 to US$2 million, under the guise of being a government minister and declaring that to qualify, persons were expected to pay fees ranging from US$550 to US$50,000 (Wong 2021). The data breach of Jamaica's JamCOVID app, which left exposed quarantine orders for more than half-a-million travellers to the island, is another example of the lack of preparedness of Caribbean governments as the pandemic accelerated internet usage without accompanying security measures (Whittaker 2021). Several regional security experts have warned that the region is underprepared for cyberattacks as criminals continue to capitalise on the digital transformation that has taken place since the pandemic (ibid).

As we have seen, Caribbean Commonwealth countries are experiencing and are likely to experience more sophisticated and advanced types of cybercrime in the coming years. To be able to combat these issues, strong national cybercrime strategies will be needed, coupled with both adequate cybercrime legislation and suitable cybercrime prevention programmes. What Caribbean countries have done so far in this area will be explored in the following section.

Measures put in place to reduce cybercrime in the Caribbean

National cybercrime measures are still not widespread in the Caribbean, which makes fighting cybercrime a daunting task. As technology advances, cybercriminals will come up with more sophisticated ways of defrauding people and businesses – making cybercrime reduction strategies a crucial part of government policy.

Globally, several policies have already been put in place to reduce the effects of cybercrime. This is exemplified through the Budapest Convention on Cybercrime, which is the first international treaty seeking to address internet and computer cybercrime by harmonising national laws, improving investigative techniques and increasing co-operation among nations (Council of Europe 2022a). As Caribbean Commonwealth countries continue to move to a more digital space, it will be crucial that more emphasis is placed on the cybercrime policies that are currently in place, as well as ensuring that leaders in cybercrime policy in the region are able to pass down their learning to other countries with less developed cybercrime policies.

Commonwealth countries with a cybersecurity strategy

Some Commonwealth countries in the Caribbean have already implemented cybersecurity strategies to help fight cybercrime. For instance, Jamaica has the National Cybersecurity Strategy, developed in 2015; Trinidad and Tobago has a National Cybersecurity Strategy, developed in 2012; and Belize has its National Cybersecurity Strategy – Towards A Secure Cyberspace 2020–2023. These countries have all instituted cybersecurity strategies to strengthen technical measures, improve legal and regulatory frameworks, and raise public awareness, as well as implementing education campaigns to help ensure the confidence of citizens in cyberspace. These three countries are therefore ahead of other Commonwealth Caribbean states due to their creation of national policies and plans on cybercrime, as these documented plans help to provide a structure towards achieving the goal or objectives of protecting their nations against cyberattacks.

Jamaica's cybersecurity strategy focuses on establishing a framework built around public education and awareness, human resource and capacity building, legal and regulatory reforms within the legislative landscape, and technical measures to support resilient cybersecurity in the country. As a result, Jamaica's strategy represents a high-level approach to cybersecurity by establishing a set of national objectives and priorities that must be met within a specific timeframe. Leadership, the protection of fundamental rights and freedoms, innovation and business development, risk management, shared responsibility, and sustainable resources are among the strategy's guiding principles. Because of their interconnectedness and the shared goal of promoting a resilient Jamaican economy on all fronts, the National Cybersecurity Strategy is implemented alongside other national development plans such as its Vision 2030 – National Development Plan, National ICT Policy and National Security Policy. The country is also leading the charge to significantly improve the Caribbean's response in tackling existing and emerging cybersecurity threats, having undertaken, in 2021, a Strategic Cybersecurity Training Needs Assessment. This will serve to identify the cybersecurity knowledge and skills required to deliver and sustain strategic responses to combat malicious cyber activities across the region.

Trinidad and Tobago's cybersecurity strategy focuses on five (5) key areas: creating an appropriate governance framework for cybersecurity; developing national incident management capabilities; developing government, civil and private industry collaborative relationships that work to effectively manage cyber risk and protect cyberspace; promoting a national culture of cybersecurity consistent with United Nations General Assembly Resolutions 57/239 entitled 'Creation of a global culture of cyber security' and 58/199 entitled 'Creation of a global culture of cyber security and the protection of critical information infrastructures'; and deterring cybercrime. The strategy aims to create a secure digital environment in which all users can fully enjoy the benefits of the internet. The country believes that the strategy will create a safe, secure and resilient cyber environment based on collaboration among all key stakeholders, allowing ICT to be used for the prosperity of all.

Belize's strategy, on the other hand, is focused on creating a secure and trustworthy digital environment that will aid in the promotion of economic growth and social inclusion in the Belize economy. The strategy was developed in collaboration with the government and other key stakeholders to provide guidance on key actions to be taken to improve Belize's overall preparedness and responsiveness to cybercriminal threats. Belize recognises that cybersecurity cannot be implemented in isolation and that it must be considered in the context of other policy decisions and national initiatives, such as the National Sustainable Tourism Master Plan 2030 and the National Growth and Sustainable Development Strategy 2016–2019, among others.

It will be crucial for these three Commonwealth Caribbean countries that these strategies do not remain documents exclusively, but that implementation also takes place in order to execute these cybercrime strategies.

Commonwealth countries currently working on a cybersecurity strategy and cybercrime legislation

Antigua and Barbuda is working on plans to update the cybersecurity legislature implemented in 2013, with an emphasis on widening the scope of cybercriminal activities. The new draft on ICT policies focuses on plans to create an independent regulatory authority and regulate the ICT space for safe and secure use of the internet and protection of intellectual property. Barbados, meanwhile, initiated its Data Protection Act (2019) in March 2021 and is currently focusing on updating its cybercrime legislation in accordance with the Budapest Convention on Cybercrime. Barbados is also currently discussing a draft bill on cybercrime with support from the Octopus Project of the Council of Europe. This bill is expected to be an update to the current Computer Misuse Act established in 2005.

In the Commonwealth of Dominica, legislation on computer and computer-related crimes has been established. In 2014, the Minister for Information Technology announced that the government intended to develop a cybersecurity strategy and would seek accession to the Budapest Convention on Cybercrime. However, this national cybersecurity strategy has been in the development stages since 2014 and has yet to be enacted. Nonetheless, the Government of Dominica is making significant strides to upgrade its resilience against potential cybercrimes by partnering with international organisations to achieve its goals. Grenada created a National Cyber Security Incident Response Team in 2022, with the aim of advising and supporting the government and the population on cyber-dependent crimes. Despite Grenada having an Electronic Crimes Bill, established in 2013 and reformed in 2016 and 2017, it is yet to develop a national cybersecurity strategy.

Other countries – such as St Vincent and the Grenadines (St Vincent and the Grenadines Cybercrime Act, 2016), Saint Lucia (Computer Misuse Act, 2008) and others listed in Table 3 – have cybercrime acts but are yet to proceed with discussions on national cybercrime strategies. With all Caribbean Commonwealth countries having implemented some form of cybercrime legislation, this demonstrates the willingness of these countries to tackle cybercrime across jurisdictions. A summary of cybercrime laws implemented in the Commonwealth Caribbean is presented in Table 3.

Table 3. Cybercrime laws in the Caribbean Commonwealth region

Caribbean country	Cybercrime laws
Antigua and Barbuda	Electronic Crimes Act, 2018
Bahamas, The	Computer Misuse Act (CMA), 2003
Barbados	Computer Misuse Act, 2005
Belize	Computer Misuse Act, 1996
Dominica	Computer And Computer Related Crimes Act, 2005
Grenada	Electronic Crimes Act, 2013
Guyana	Cyber Crime Act, 2018
Jamaica	Cybercrimes Act, 2015
St Kitts and Nevis	Electronic Crimes Act, 2009
Saint Lucia	Computer Misuse Act, Cap 8.14
St Vincent and the Grenadines	St Vincent and the Grenadines Cybercrime Act, 2016
Trinidad and Tobago	The Computer Misuse Act, 2000

Source: G5 Cybersecurity 2021

At the regional level, the Caribbean Community and Common Market (CARICOM) established an Implementation Agency for Crime and Security (IMPACS) in July 2006 and released its inaugural Cyber Security and Cybercrime Action Plan (CCSCAP). The action plan seeks to address the cybersecurity vulnerabilities in each participating Caribbean country and to establish a practical, harmonised standard of practices, systems and expertise for cybersecurity. Furthermore, it aims to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of cybercrime to take place. In 2019, IMPACS's objectives were given a boost when it secured funding from the European Union (EU) to undertake a 'Capacity Development' project across CARICOM nations. However, at the time of writing there had yet to be any public information concerning the success of CCSCAP within the Caribbean region.

Furthermore, the World Bank instituted the World Bank Caribbean Digital Transformation Project 2020–2026 to improve cybersecurity, data protection and privacy by reviewing and updating regional and national cybersecurity regulations and legislations. Finally, the Council of Europe held a conference on Cybercrime Strategies and Policies in 2019, with the aim of encouraging Caribbean countries to ratify the Budapest Convention in order for countries' legislation to be consistent with international cybercrime law.

The future of cybercrime strategies in the Caribbean

Following the expansion of the internet, an increase in broadband technologies and continued economic advancements, cybercrime has increased rapidly across the Caribbean region. The rise of cybercriminal activity can be attributed to increased levels of connectivity, remote working, reliance on technology and automation, which mean the risk of attacks is rising rapidly. This, coupled with an increasingly professionalised, specialised and collaborative underground supply chain of cybercriminals, suggests that growth in cyber criminality is likely to increase across the Caribbean. In order to limit the danger posed by cybersecurity issues and digitally enabled crime in the region, initiatives must focus on addressing the threats and vulnerabilities these states face. This should include improving technical standards and infrastructure, fostering national and regional regulations that would enforce penalties on cybercrime offenders, improving public awareness, and increasing both regional and international co-operation. To be able to achieve this, co-operation between key stakeholders is necessary. Given the multisectoral and cross/multinational impacts of cybercrime, an effective response to the issue will require collaboration at the cross-sectoral, bilateral and multinational levels. A discussion of the role of key stakeholders in fighting cybercrime across these different areas going forward is therefore provided below. Lessons learnt from other regions are also provided.

Government and the police

The role of government in the Caribbean Commonwealth is predominantly to provide both a legislative and regulatory environment that protects businesses and citizens from cybercrime. This includes collaboration on legislation at the international level to allow for harmonised legislation for cross-border, international crimes that need an international response. This is especially crucial in the Caribbean, given the interconnected nature of cybercrimes across the region. Furthermore, legislation can also consider criminalising specific types of cybercrime that have caused problems at the national or regional levels to demonstrate the legislator's willingness to address the issue (Global Action on Cybercrime 2019). This legislation also needs to be sufficiently abstract so that it is able to endure over time as cybercriminals evolve their operations. This way of creating regulation has been exemplified in Jamaica, as its legal and regulatory framework aims to carry out periodic reviews of existing laws to ensure parity with the dynamic nature of cybercrimes.

It is also crucial that Caribbean governments invest in institutions that permit action against cyberthreats, such as funding towards the development of remedial and preventative measures. This includes the police in the Caribbean, as they play a key role in cybersecurity. However, this will require new skills and competencies that extend well beyond those needed for traditional policing. Training will be essential for the police to maintain pace with evolving areas of cybercrime and capacity building in this respect will be crucial. This could take place at the regional level, given the limited resources of certain Commonwealth Caribbean countries as well as the overlap of many types of cybercrime across the region. Such training has already taken place, with a collaboration between the Commonwealth Secretariat and the Caribbean Community Implementation Agency for Crime and Security providing a four-day training session in Barbados to teach Caribbean police and legal experts how to use electronic evidence in cybercrime cases (Commonwealth Secretariat 2016).

The private sector

Given the limited resources of Caribbean Commonwealth countries, the private sector can also play a role in mitigating the impacts of cybercrime. Overall, the private sector in the region must protect itself and its clients from threats by ensuring basic cybersecurity measures are in place. Furthermore, in the Caribbean context, because attacks usually have an impact at the regional level, making sure several governments work together to ensure the best possible sharing of knowledge among all countries on the types of evidence that can be provided by the private sector will be crucial. The creation of private–public co-operative forums and joint tasks force initiatives will also provide robust preventative and response measures to cybercrime in the region. In addition to this, it would be worthwhile for private sector companies to adhere to international best practice standards, such as ISO/IEC 27032, as well as establish an industry co-regulatory approach such as the development of industry standards in relation to mandatory cyber-hygiene practices.

Although there is reference to ensuring the private sector is involved in cybersecurity across Caribbean countries within national cyber security strategies, the implementation of this seems to be lacking. However, one country leading the way in this area is The Bahamas, which has seen top IT professionals across a range of sectors participate in the government's first national cybersecurity assessment session, helping to provide a unique perspective on cybercrime issues (Eyewitness News 2021).

Prevention strategies from citizens and civil society

The involvement of citizens and civil society will also be crucial in combatting cybercrime going forward. Ultimately, citizens will be the ones who are the victims of cybercrime as not only will they suffer directly from these crimes, but also from the loss of income due to the closure of companies and lost opportunities and investments if the Caribbean is not seen as a place where business can take place safely. Citizens who have been victimised are also able to fully understand these cybercrimes and can therefore provide a unique perspective when it comes to carrying out public awareness campaigns or establishing prevention strategies in collaboration with civil society. This is increasingly important, given the high levels of digitally connected citizens across the Caribbean region. Consideration should also be given to the use of sensitisation sessions for different age groups: for example, cyberbullying and social media safety for schools, online business safety for micro and small and medium-sized enterprises (MSMEs) and sole traders online, as well as general online safety for members of the public.

Evidence of collaboration between governments, civil society and citizens around cybercrime has already been seen in Belize, where a cross-section of national stakeholders worked together in order to develop the National Cybersecurity Strategy, 2020–2023 (Council of Europe 2022b).

International partners

Across the Caribbean, we have seen examples of successful cybercrime strategies and interventions, highlighting the importance of international partnerships in this area as Caribbean states can learn from each other. Furthermore, evidence has shown throughout this paper that in some cases, cybercrimes can be interconnected at the regional level, making a further case for international co-operation. The harmonisation of laws, co-ordinated investigative techniques, and improved access and collaboration with respect to electronic evidence are some of the ways that Caribbean countries will be able to improve this co-operation to reduce cybercrime. The CARICOM Cyber Security and Cybercrime Action Plan is an excellent example of this co-operation at the regional level as a co-ordinated framework has been created, helping to avoid duplication of effort in reducing cybersecurity issues and to disseminate lessons learnt from larger, or more technically mature, countries to smaller states. It may also be worthwhile considering greater enforcement of cross-border co-operation through mutual legal assistance treaties between different Caribbean states. Finally, the involvement of Caribbean Commonwealth states in the current international discourse at the UN level within the Open-Ended Working Group (OEWG) on the use of ICTs could be a crucial way to ensure that Caribbean countries are actively involved in developing rules, norms and principles of responsible behaviour in this area and helping them to understand the extent of potential threats in the sphere of information security.

We have also seen evidence of cyberattacks in the Caribbean being carried out far beyond its regional borders and therefore co-operation further afield is necessary. Cybercriminals will often seek out victims in a different jurisdiction to where they are based to reduce the evidence against them being readily available. Going forward, as technologies improve, these types of cyberattacks will also become easier to carry out. The US, the EU and the United Kingdom (UK) have already provided international support and capacity building by hosting, in collaboration with several Caribbean countries, cyber capacity workshops and legislation working groups to help strengthen cybercrime policies.

Lessons learnt: Five Eyes

As we have established, collaboration with international partners is essential for Caribbean Commonwealth countries to be able to tackle cybercrime effectively. In addition, although Caribbean governments do not have equivalent resources to those of advanced states, there are still lessons that can be learnt from their approaches and interventions to allow for maximum impact. This is especially the case for 'Five Eyes', which is an intelligence alliance between the world's five leading cybersecurity authorities, Australia, Canada, New Zealand, the UK, and the US. Their forward-thinking cyber strategies can help Caribbean states develop long-term policies to address cybersecurity challenges in the future.

The first lesson from these strategies is the extensive research that went into developing them, including extensive public consultation processes that included a diverse range of stakeholders such as academics, technology experts and business leaders, to name a few. For example, Public Safety Canada received more than 2,000 comment submissions for the development of its 2019–2024 Cyber Security Strategy (Public Safety Canada 2019). Second, the importance of protecting critical national infrastructure is also highlighted as a priority throughout all five cybersecurity strategies. This is especially highlighted in New Zealand's cybersecurity strategy, given several attacks against critical infrastructure that were a result of hacking tools becoming more accessible and public services being moved online. Finally, identifying key threat groups such as nation-states, foreign state-sponsored actors and proxy actors will help towards ensuring adequate measures are put in place before attacks occur. The UK has highlighted this in its cyber strategy, suggesting that as cyber warfare is to become an essential part of armed conflicts, a country's defence capabilities need to match this trend.

Learning from these countries and understanding these future trends will be essential for Caribbean Commonwealth countries to remain resilient in the face of growing cyberattacks.

Conclusion

If Caribbean Commonwealth countries do not take adequate measures to protect themselves and their citizens from cybercrime, the impact is likely to be large. As discussed, cybercrime tends to affect small countries more than larger countries due to the larger countries' ability to cushion the effect better at the national level compared to a smaller state, making Caribbean Commonwealth countries particularly vulnerable.

This is especially true given the increased levels of internet usage, high levels of mobile cellular subscriptions and a lack of secure internet servers in certain Caribbean Commonwealth countries, which all contribute to cybersecurity risks. Organised crime groups in the region have already started to exploit these developments through a range of methods. These include cyber-enabled crimes such as phishing, skimming and the use of social media, but also cyber-dependent crime including hacking, ransomware and through Central Bank Digital Currencies. The COVID-19 crisis has accelerated changes that were already underway in the online criminal economy, with implications for cybercrime activities in the Caribbean.

To address these issues, some Commonwealth countries have already put in place measures to curb cybercriminal activity. Jamaica, Trinidad and Tobago, and Belize have setup national cybersecurity strategies, aiming to improve legal and regulatory frameworks, strengthen technical measures and raise public awareness. All Caribbean Commonwealth countries have some form of cybercrime law, demonstrating their willingness to tackle cybercrime across jurisdictions. At the regional level, CARICOM IMPACS has brought together Caribbean nations to address cybersecurity vulnerabilities and establish practical, harmonised standards of practices, systems and expertise for cybersecurity.

For Caribbean Commonwealth countries to ensure they continue to be protected in the face of increasing cybercrime threats, building on current initiatives will be necessary. This includes ensuring that governments collaborate on legislation at the international level to allow for harmonised legislation for cross-border, international crimes that need an international response. Furthermore, training will be essential if police forces are to be able to keep up with evolving areas of cybercrime. Given the limited resources of Caribbean Commonwealth countries, the private sector can also play a role in mitigating the impacts of cybercrime by ensuring knowledge sharing of evidence takes place at the regional level. The involvement of citizens and civil society will also be crucial going forward, as citizens who have been victimised are able to fully understand these crimes and can therefore provide a unique perspective and establish prevention strategies in collaboration with civil society. Finally, international partnerships will be necessary for Caribbean Commonwealth states, as this will allow countries to learn from one another while at the same time helping to combat cybercrime at the regional level.

Finally, to ensure Caribbean Commonwealth countries are forward looking in their approaches, it is important for them to pay attention to leading cybersecurity authorities, such as Five Eyes, for lessons learnt and guidance. This will mean that Caribbean countries' strategies are prepared for the long term and that they continue to adapt and innovate to protect and promote their cyberspaces.

References

Barrett, L (2022), 'Massy's ransomware attack exposes consumers and companies', eSponsored, Jamaica Gleaner, available at: https://jamaica-gleaner.com/article/esponsored/20221017/massys-ransomware-attack-exposes-consumers-and-companies (accessed 15 August 2022).

Bank of International Settlements (2021), 'BIS Innovation Hub work on central bank digital currency (CBDC)', available at: www.bis.org/about/bisih/topics/cbdc.htm (accessed 15 August 2022).

Breaking Belize News (2022), 'Fines and suspended sentences for men who pled guilty to making gang video', Belize News and Opinion, available at: www.breakingbelizenews.com/2022/10/12/fines-and-suspended-sentences-for-men-who-pled-guilty-to-making-gang-video/ (accessed 3 October 2022).

Bridglal, C (2020), 'Ansa McAl IT systems recovery "largely complete" after hack attack', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2020/10/27/ansa-mcal-it-systems-recovery-largely-complete-after-hack-attack/ (accessed 20 October 2022).

Caribbean Community (CARICOM) (2015), 'St Lucia tightens cyber security after hacking of SVG site', available at: https://caricom.org/st-lucia-tightens-cyber-security-after-hacking-of-svg-site/ (accessed 15 August 2022).

Check Point Research (2022a), 'Cyber Attacks Increased 50% Year over Year', available at: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (accessed 15 August 2022).

Check Point Research (2022b), 'Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware', available at: https://blog.checkpoint.com/2022/07/26/check-point-research-weekly-cyber-attacks-increased-by-32-year-over-year-1-out-of-40-organizations-impacted-by-ransomware-2/ (accessed 15 August 2022).

Commonwealth Secretariat (2016), 'Commonwealth cybercrime experts in Barbados call for robust cybersecurity', The Commonwealth, available at: https://thecommonwealth.org/news/commonwealth-cybercrime-experts-barbados-call-robust-cybersecurity (accessed 3 October 2022).

Comply Advantage (2022), 'AML In The Caribbean: UBOs and Shell Companies', available at: https://complyadvantage.com/insights/aml-carribbean-ubos-shell-companies/ (accessed 20 October 2022).

Council of Europe (2022a), 'The Budapest Convention', Cybercrime, available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 3 November 2022).

Council of Europe (2022b), 'Status regarding Budapest Convention', available at: www.coe.int/ru/web/octopus/-/belize?inheritRedirect=true (accessed 3 October 2022).

Cybersecurity Ventures (2022), *Boardroom Cybersecurity 2022 Report*, available at: https://cybersecurityventures.com/boardroom-cybersecurity-report/ (accessed 15 August 2022).

Douglas, S (2022), 'Cox: Human traffickers target youngsters on social media', *Trinidad and Tobago Newsday*, PBJ Learning, available at: https://pbjlearning.com/2022/09/07/cox-human-traffickers-target-youngsters-on-social-media-trinidad-and-tobago-newsday/ (accessed 3 October 2022).

Eleutheran News (2015), 'Ministry of Tourism updates on the hacking of bahamas.com', available at: https://eleutheranews.com/?p=4719 (accessed 20 October 2022).

Europol (2020), 'Catching the virus: cybercrime, disinformation and the COVID-19 pandemic', 3 April, 3, available at: www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_class="•-No-break">pandemic_0.pdf (accessed 3 November 2022).

Eyewitness News (2021), 'Top IT professionals participate in govt's first-ever national cybersecurity assessment session', Eyewitness News, available at: https://ewnews.com/top-it-professionals-participate-in-govts-first-ever-national-cybersecurity-assessment-session (accessed 15 August 2022).

G5 Cybersecurity (2021), *2021 Caribbean Cyber Security and Privacy (CSPR) Report*, available at: https://g5cybersecurity.com/downloads/reports/G5CS-2021-Caribbean-Cyber-Security-and-Privacy-Report-CSPR.pdf (accessed 15 August 2022).

George, J (2018), 'Organized Crime and Cyber Crime in Latin America and the Caribbean', available at: www.linkedin.com/pulse/organized-crime-cyber-latin-america-caribbean-jaevon-george-bsc/?trk=articles_directory (accessed 15 August 2022).

Global Action on Cybercrime (2019), Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community, available at: https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c (accessed 15 August 2022).

Global Initiative (2020a), Global Organized Crime Index – Jamaica, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_jamaica.pdf (accessed 3 November 2022).

Global Initiative (2020b), Global Organized Crime Index – Trinidad and Tobago, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_trinidad_and_tobago.pdf (accessed 3 November 2022).

Global Initiative (2020c), Global Organized Crime Index – Dominica, available at: https://ocindex.net/assets/downloads/english/ocindex_profile_guyana.pdf (accessed 3 November 2022).

Guyana Standard (2020), 'Police warn of online scam targeting women', available at: www.guyanastandard.com/2020/11/26/police-warn-of-online-scam-targeting-women/ (accessed 20 October 2022).

Hamilton-Davis, R (2023), 'Amcham: Crime, ease of doing business among top concerns', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2023/01/19/amcham-crime-ease-of-doing-business-among-top-concerns/ (accessed 3 November 2022).

Home Office (2013), 'Cyber-dependent crimes', chapter 1 in *Cyber crime: A review of the evidence Research Report 75*, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf (accessed 15 August 2022).

InSight Crime (2018), 'Caribbean Profile', InSight Crime, available at: https://insightcrime.org/caribbean-organized-crime-news/caribbean/ (accessed 18 October 2022).

International Organization for Migration (IOM) (2015), *Exploratory Assessment of Trafficking in Persons in the Caribbean Region: The Bahamas, Barbados, Guyana, Jamaica, The Netherlands Antilles, St. Lucia, Suriname and Trinidad and Tobago,* second edition, available at: https://publications.iom.int/system/files/pdf/exploratory_assessment2.pdf (accessed 15 August 2022).

Katz, C (2015), *An Introduction to the Gang Problem in the Caribbean*, available at: www.researchgate.net/publication/282981024_An_Introduction_to_the_Gang_Problem_in_the_Caribbean (accessed 15 August 2022).

Kurmi, S (2022), 'Investing In Cryptocurrency', Forbes Advisor UK, available at: www.forbes.com/uk/advisor/investing/cryptocurrency/ (accessed 3 November 2022).

Mckenzie, R (2022), 'Suspects arrested in connection with $45 million theft at JMMB', Sleek Jamaica Media, available at: https://sleekjamaica.com/suspects-arrested-in-connection-with-45-million-theft-at-jmmb/ (accessed 3 November 2022).

Moore, M (2017), *Cybersecurity Breaches and Issues Surrounding Online Threat Protection*, a volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, IGI Global, USA.

National Bank of Dominica (2021), 'Statement on SPAM Emails', National Bank of Dominica Ltd, available at: https://nbdominica.com/statement-on-spam-emails/ (accessed 24 October 2022).

National Cyber Security Centre (2017), 'Cybercrime – understanding the online business model', available at: www.ncsc.gov.uk/files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf (accessed 15 August 2022).

Oré, D (2020), 'Latin American crime cartels turn to cryptocurrencies for money laundering', US, available at: www.reuters.com/article/mexico-bitcoin-insight-idUSKBN28I1KD (accessed 15 August 2022).

Popplewell, G (2019), 'Guy Fawkes makes cameo appearance on hacked Trinidad and Tobago government websites', *Global Voices*, available at: https://globalvoices.org/2019/07/26/guy-fawkes-makes-cameo-appearance-on-hacked-trinidad-and-tobago-government-websites/ (accessed 20 October 2022).

Public Safety Canada (2019), National Cyber Security Strategy, available at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf (accessed 3 October 2022).

Reitano, T and M Shaw (2021), *Criminal Contagion: How Mafias, Gangsters and Scammers Profit from a Pandemic*, Hurst Publishers, United Kingdom.

Superville, S (2021), 'Bank card skimming concern for cybersecurity in Trinidad and Tobago', *Trinidad and Tobago Newsday*, available at: https://newsday.co.tt/2021/10/24/bank-card-skimming-concern-for-cybersecurity-in-trinidad-and-tobago/ (accessed 3 October 2022).

Trinidad and Tobago Guardian (2021), 'FIUTT detects $2.3 million loss from victims of romance scams', available at: https://guardian.co.tt/news/fiutt-detects-23-million-loss-from-victims-of-romance-scams-6.2.1379265.39b80d75c7 (accessed 15 August 2022).

UN Office on Drugs and Crime (UNODC) (2012), 'Digest of Organized Crime Cases: A compilation of cases with commentaries and lessons learned', available at: www.unodc.org/documents/organized-crime/EnglishDigest_Final301012_30102012.pdf (accessed 15 August 2022).

UNODC (2013), 'Draft Comprehensive Study on Cybercrime', available at: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 15 August 2022).

UNODC (2019), 'Organized Crime / Cybercrime Module 13 Key Issues: Criminal Groups Engaging in Cyber Organized Crime', available at: www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html (accessed 15 August 2022).

Verizon (2022), *Verizon's 2022 Data Breach Investigations Report*, available at: www.verizon.com/business/resources/reports/dbir/ (accessed 15 August 2022).

World Development Indicators (WDI) (2022a), World Development Indicators (WDI), International Bank for Reconstruction and Development/The World Bank, Washington, DC, available at: https://databank.worldbank.org/source/world-development-indicators

WDI (2022b), 'Internet Penetration Over Time', available at: https://databank.worldbank.org/Internet-Penetration-over-time/id/3bdec3cd (accessed 15 August 2022).

White House (2022), National Drug Control Strategy Caribbean Border Counternarcotics Strategy, available at: www.whitehouse.gov/wp-content/uploads/2022/04/Caribbean-Border-Counter-Narcotics-2022Strategy.pdf (accessed 18 October 2022).

Whittaker, Z (2021), 'How Jamaica failed to handle its JamCOVID scandal', available at: https://techcrunch.com/2021/04/03/jamaica-jamcovid-amber-group/?guccounter=1 (accessed 18 October 2022).

Wint, A (2003), *Competitiveness in Small Developing Economies*, UWI Press, Kingston.

Wilson-Harris, N (2019). 'Cyber thieves run rampant - Jamaica suffering billions in losses from online crime', Jamaica Gleaner, available at: https://jamaica-gleaner.com/article/lead-stories/20190630/cyber-thieves-run-rampant-jamaica-suffering-billions-losses-online (accessed 22 February 2023).

Wong, M (2021), 'Grenadians urged not to fall for COVID assistance scams online', Loop News, available at: https://caribbean.loopnews.com/content/grenadians-urged-not-fall-covid-assistance-scams-online (accessed 20 October 2022)

Commonwealth Cybercrime Journal \ 111
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Data Security Concerns Raised by 'Bring Your Own Device' in Corporate Organisations' Hybrid and Remote Work Environments in Nigeria

Rotimi Ogunyemi[1] and Akintunde Idowu[2]

Abstract

The perceived benefits of increased productivity, employee efficiency and work flexibility have given rise to the phenomenon known as 'bring your own device' (BYOD), which permits employees of an organisation to complete their tasks or processes on their own personal devices. The COVID-19 pandemic accelerated this trend, particularly as the shift to hybrid and remote work intensified. Major organisations have pushed for the adjustment of their personnel, procedures and cultures to the new reality. The fact that employees can access organisational data from their own devices at any time and from any location increases the likelihood of unauthorised access to corporate data. Finding secure technologies for conducting confidential meetings in a remote workspace and managing confidential data outside of a remote location has been difficult. The vulnerabilities include, among others, phishing email attacks, unauthorised access through insecure remote-access tools and hacking of video conference tools. As remote work tools must be protected, periodic risk assessments and routine monitoring are required to safeguard the privacy and integrity of an organisation's information assets and resources. This paper seeks to investigate the role of cybersecurity in general; data privacy and security challenges posed by BYOD using Nigeria as a case study; cybersecurity policy recommendations for remote and hybrid work; and the implementation of a secure BYOD structure.

[1] Technology Lawyer; Managing Partner, Johnson & Wilner LLP, Nigeria (Formerly Bayo Ogunyemi & Co.); President, Spindlar Cyberlaw Centre (Lagos, Nigeria). linkedin.com/in/rotimiogunyemi

[2] Intellectual Property and Information Technology Lawyer, Johnson & Wilner LLP, Nigeria. linkedin.com/in/akintundeidowu

Introduction

According to available data, 83 per cent of companies allow employees to use their own devices, such as laptops, tablets and smartphones, for business purposes.[3] The results of a recent survey indicate that 95 per cent of employers have adopted 'bring your own device' (BYOD) due to technological advancements and the perceived costs of providing their workforce with secured devices, and that 57 per cent of employees prefer the convenience of keeping track of personal and work-related items on a single device.[4] It is, therefore, no surprise that the global BYOD market size is expected to grow by US$69.07 billion from 2021 to 2026.[5]

Bring your own device or BYOD is a policy in which employees use personally selected and purchased devices to perform work for their employer via remote intranet access.[6] This includes the use of mobile devices such as smartphones, tablets, laptops and personal computers. The goal of a BYOD scheme is to enable the employee to be more productive and efficient by selecting a device that best suits his or her preferences and work purposes, while ensuring data integrity and protecting the organisation's data from leakage and loss.[7]

According to joint research, approximately 88 per cent of all data breaches are due to employee error.[8] For example, it was reported that the personal information of about 30,000 customers of the South Korean cryptocurrency exchange Bithumb was recently exposed when a Bithumb employee's home computer was hacked.[9] A 2020 report[10] indicates that 62 per cent of businesses experienced **phishing and social engineering** attacks[11] and 91 per cent of this type of cybercrime is said to begin with malicious email

[3] Zippia (2022), '26 surprising BYOD statistics [2022]: BYOD trends in the workplace', Zippia.com, 17 October, available at: https://www.zippia.com/advice/byod-statistics/ (accessed 2 November 2022).

[4] Samsung (no date), 'Maximizing Mobile Value', White Paper, Samsung Business, available at: www.samsung.com/us/business/short-form/maximizing-mobile-value-2022/ accessed 11 September 2022. p.2. The survey was conducted between 2021 and 2022 with 500 executives and 1,000 employees in the United States.

[5] Technavio (2022), 'Bring your own Device (BYOD) Market by End-user and Geography – Forecast and Analysis 2022–2026', Technavio.com. September, available at: https://www.technavio.com/talk-to-us?report=IRTNTR74271&type=sample&rfs=epd&src=report&utm_source=prnewswire&utm_medium=pressrelease+&utm_campaign=t42dtcs_rfs1_wk41_2022_007&utm_content=IRTNTR74271 accessed 2 November 2022.

[6] Cavoukian, A (2013) 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' Information and Privacy Commissioner Ontario, Canada, retrieved from https://silo.tips/download/byod-bring-your-own-device-is-your-organization-ready accessed 2 November 2022.

[7] Ibid.

[8] Tessian (no date), 'Understand the mistakes that compromise your company's security', available at: https://www.tessian.com/research/the-psychology-of-human-error/

[9] Yonhap News Agency (2017), 'S. Korea probes cyberattack on digital currency exchange', 3 July, available at: https://en.yna.co.kr/view/AEN20170703010400320 accessed 1 November 2022.

[10] T-Mobile for Business (2020) *The T-Mobile for Business 2020 Workplace Mobility Report*, available at: https://www.t-mobile.com/content/dam/tfb/pdf/T-Mobile-for-Business-2020-Workplace-Mobility-Report.pdf?icid=TFB_TMO_P_TFBFTRWRKS_7LCBNVDVYBXY27WF321599 accessed 1 November 2022.

[11] See discussion of these terms on page 5.

links. Thus, although BYOD devices create business transformation, the phenomenon is at the heart of data breaches, cybercrime and network attacks and poses arguably the largest risk to enterprise security.

Given that data security is essential to information privacy, this poses a significant threat. Indeed, security is a prerequisite for privacy.[12] There should be no gaps in protection or accountability for secure storage or transmission, regardless of whether the information is stored on a mobile device, in a database or in the cloud. As organisations' operations have become more data-intensive, network-dependent and accessible than ever before, ensuring full lifecycle protection has become a formidable obstacle.[13] The proliferation of mobile devices such as laptops, smartphones, tablets, USB drives and portable storage media, as well as the increasing use of personal mobile devices for business purposes, necessitates a fundamental revaluation of how to best protect end-to-end the sensitive data of the modern enterprise.[14]

As information processing technologies, business practices and networked architectures become increasingly complex and critical for organisational operations, it is more important than ever to anticipate security risks as early as possible and to mitigate those risks by defaulting to strong policy, and technical, administrative and physical security practices. Several intersecting growth trends are pressuring companies to let employees use their own devices and connect them to corporate networks and systems. Consumer adoption of new mobile device brands, the rapid evolution of device capabilities, as well as of cloud and virtualisation technologies, the explosive growth of mobile applications, and a growing tech-savvy population adept at using mobile technologies are a few of these factors.[15] Although working on a mobile device offers many benefits to employees and employers, this blurring of personal and business use of BYODs raises many data security and cybersecurity concerns that, if not properly addressed, may result in data breaches, turning the many BYOD benefits into losses for organisations.[16]

Prior literature reviews suggest that data security issues in BYOD are under-researched, as they are relatively young compared to other data security issues. This paper draws the attention of corporate organisations to implications they should be aware of in order to increase safeguards against threats targeting BYOD initiatives. It also focuses on the legal implications of BYOD schemes on real-life business issues and as well as how the judiciary approaches the determination of BYOD cases in corporate organisations. This paper seeks to answer questions such as:

- What are the data security issues associated with the processing of employees' personal data on BYODs for work-related purposes?

[12] Cavoukian, 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' [2] (n 1).

[13] Ibid.

[14] Ibid.

[15] Ibid, p.3.

[16] Ibid.

- What is the judiciary's approach to determining BYOD cases in corporate organisations?
- What are the legal measures, including policies and strategies, for implementing BYOD schemes?

This paper will seek to produce an assessment of BYOD issues that can also serve as a template for organisations. It will begin with a conceptual analysis of the BYOD schemes by describing the relevant law and carrying out an analysis of previous literature. It will also examine the data security issues pertaining to the processing of employees' personal data for work-related purposes. Furthermore, it will attempt to provide an analysis of the judiciary's approach to determining BYOD cases in corporate organisations by comparing case laws in the United Kingdom (UK), the United States (US), Canada and Europe with Nigeria, outlining the challenges this approach presents and demonstrating inconsistencies in Nigerian jurisprudence. Just like Nigeria, the UK and the US are generally considered common law countries (while Canada and Europe have a mix of both common law and civil law systems) and therefore provide a suitable basis for comparison.

Conceptual analysis of BYOD schemes

The terms BYOD, CYOD, COPE, and COBO are encountered by anyone researching enterprise mobility (plus a few more). BYOD stands for 'bring your own device', CYOD for 'choose your own device', COPE for 'company owned/personally enabled', and COBO for 'company owned/business only'. There is little agreement on their meaning, but they are all similar concepts.[17] BYOD and CYOD involve smartphone-based integration and access, while COPE and COBO involve company-owned and -controlled devices.[18] The *Wired* blog[19] provides a helpful summary of the three factors that determine a device's category.

1. Who chooses the device, who pays for the device and the cellular connectivity service?
2. Who is responsible for managing and providing support for the device?
3. How crucial is the device's integration with daily workflow?

As will be discovered later in this article, the answers to these questions are useful for determining the numerous questions of liability for security and privacy risks associated with the use of BYOD devices for enterprise applications. Yet the issue of ownership may not be straightforward, especially when the employer contributes to the device's cost and/or compensates the employee for its use. Therefore, businesses must safeguard their data to reduce their liability exposure. Employers should consider the responses to

[17] Wired (2018), 'BYOD, CYOD, COPE, COBO — What Do They Really Mean?', available at: https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/ (accessed 2 November 2022).

[18] Ibid.

[19] Ibid.

the three factors when drafting policies that serve as a reminder to employees that all company data belongs to the employer, while the issue of device and content ownership must be made explicit.

Data security risks associated with BYOD in remote and hybrid work

Bring your own device is a trend with both risks and benefits. While the benefits may include potential cost savings as employees invest in their own devices, a solution to the 'two pocket problem' that allows employees to carry one device instead of two (one for work and one for personal use), an increase in employee engagement and productivity because employees use devices they desire and are familiar with, and enhanced recruitment strategies by attracting candidates with technological expertise, the risks for employers appears to far outweigh the benefits. Of many types of attacks affecting BYOD devices, the notable risks include: data loss due to device loss, phishing, spyware attacks and malware attacks, network attacks, and Zoom bombing.[20]

1. Data loss due to device loss

Smart devices contain large amounts of data covering different services such as emails, contacts, social media, credit card information, etc. When an employee connects his/her personal devices to a corporate network, he/she makes it easier for hackers to access employee information, company data and the corporate directory. If this device is stolen, it leaves the owner vulnerable and gives room for the exploitation of corporate networks and data. Once inside, a hacker can hide in the corporate network, steal desired information and monitor network activity, particularly outbound traffic. This eventually leads to the organisation suffering data loss or data breach.

2. Phishing, spyware attacks and malware attacks

Phishing is a form of social engineering commonly used to steal user data, including login credentials and credit card information. It occurs when an attacker impersonates a trusted entity in order to deceive a victim into opening an email, instant message or text message. Phishing can have devastating consequences for employees if an attacker gains access to a company network as part of a larger attack and this may result in the attacker making unauthorised purchases, stealing funds and employee identity. In this scenario, employees are compromised as an attacker circumvents security perimeters, spreads malware within a closed environment or gains privileged access to secured data. This typically results in financial losses, and declines in market share, reputation and consumer trust in businesses.[21] Similar to phishing attacks are 'spoofing' attacks.

[20] Rai, S, P Chukwuma and R Cozart (2016), *Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices,* Auerbach Publications, pp. 54–55.

[21] Imperva (no date), 'Phishing attacks', available at: www.imperva.com/learn/application-security/phishing-attack-scam/ (accessed 4 November 2022).

Spyware, by comparison, allows an intruder to covertly obtain information from a user's computer. It can be acquired through a phishing attack. Once the user clicks on the link in the phishing attack, the spyware is installed and it monitors smart device usage, keystrokes, and is able to copy contact information or financial information. Where the smart device is connected to a corporate network, the spyware will collect all the necessary information that a hacker needs to break into the corporate network. When a single individual or corporation is targeted, the spyware attack becomes a surveillance attack. The surveillance attack may or may not be for criminal intentions. Some of these applications installed by employees contain trojan viruses, which are rogue applications that can be used to introduce advance persistent threats (APTs).

3. Network attacks

Network attacks generate additional traffic and bandwidth consumption, which can impede network performance. They include distributed denial of service (DoS), man in the middle attacks, network sniffing and ransomware. 'Ransomware' refers to software that can be maliciously installed on a computer or a network, and which is designed to block access to critical data, such as by encrypting files, until a ransom is paid. A recent report found that 71 per cent of Nigerian organisations were hit by ransomware in 2021, a higher number when compared to the previous year.[22] Another 2022 report reveals that 49 per cent of organisations that had their data encrypted paid ransoms to get their data back.[23]

4. Zoom bombing

Zoom bombing is a challenge that became prominent during the COVID-19 pandemic and has since naturalised in remote meetings. The increased use of Zoom and other videoconferencing platforms has given prominence to efforts of malicious users to sabotage classrooms and discussions in attacks that have been termed 'Zoom bombing'.[24] Some have defined this as 'gate-crashing tactics during public video conference calls' that often result in flooding the calls with disturbing images. A report by VMware Carbon Black, based on a survey of 1,002 respondents conducted in March and April 2020, estimated that 91 per cent of executives believed that cyberattacks on

[22] Guardian Nigeria (2022), 'Ransomware hits 71% of Nigerian Organisations', 4 May, available at: https://guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/ (accessed 4 November 2022).

[23] Sophos, 'State of Ransomware in Retail 2022 report', retrieved from https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-retail accessed 4 November 2023.

[24] Oxford University News Science Blog, 'FBI follows Oxford academics' guide to beat Zoom bombers' (24 April 2020) https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers accessed 24 February 2023.

their organisation increased because of remote working during the pandemic.[25] Some 85 per cent believed that their own organisation was not adequately prepared to deal with a sudden shift to working from home.[26]

Existing statutory laws and security obligations applicable to BYOD in Nigeria

In Nigeria, the laws and policies affecting bring your own device (BYOD) are mainly governed by the Nigerian Data Protection Regulation, Nigerian Cybercrime Act, Electronic Transactions Act, and the Freedom of Information Act. These Acts set out the framework for the regulation of the information and communications technology sector in Nigeria, and include provisions related to privacy, security and the protection of personal data that have a bearing on the use of personal devices for work purposes.

1. Nigerian Data Protection Regulation (NDPR)

To ensure the protection of personal data, data controllers and processors have specific security obligations, including both technical and organisational measures that increase the level of information technology (IT) security directly or indirectly. These obligations can be grouped into seven main areas of data protection: (i) data minimisation and storage limitation; (ii) data confidentiality; (iii) risk assessment and security measures; (iv) data protection by design and by default; (v) regular assessment of the effectiveness of the security measures taken; (vi) notifications, reporting obligations and mitigation measures (data breaches); and (vii) business continuity, disaster recovery and resilience.

On data minimisation and data storage limitation, the Nigerian Data Protection Regulation (NDPR) requires data controllers to ensure that a limited amount of data is obtained and processed as strictly necessary[27] ('data minimisation'); and that no data may be collected unless the employee is informed of the purpose. Furthermore, employee data should not be retained for longer than necessary[28] ('data storage limitation'). A strategy based on data minimisation and storage limitation can help mitigate the effects of data breaches caused by cyberattacks or incidents, from the perspective of cybersecurity.[29]

[25] The Daily Swig (2020), 'Remote working during coronavirus pandemic leads to rise in cyberattacks, say security professionals, 14 July; VMware (2020) *Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat*, available at: https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/

[26] Ibid

[27] Section 2.1 (b) NDPR 2019.

[28] Section 2.1(1) (c) NDPR 2019; see also Section 38 of the Cybercrime Act, which stipulates that service providers must retain traffic data and subscriber information for at least two years. In addition, Section 5 of the Credit Reporting Act of 2017 mandates that a credit bureau should keep credit information for at least six years from the date it was obtained, after which it must be archived for an additional ten years before being destroyed.

[29] See also Mantelero, A and G Vaciago (2017), 'Legal Aspects of Information Science, Data Science and Big Data', in M Dehmer and F Emmert-Streib (Eds.), *Frontiers in Data Science,* CRC Press.

The regulation requires controllers and processors to perform a Data Protection Impact Assessment (DPIA)[30] and a Data Protection Audit[31] to identify and mitigate against any data protection-related risks arising from employees' performance of work projects on their BYODs ('risk assessment'). This goes beyond data security and takes a more holistic risk-based approach, focusing on the impact of data use on the rights and freedoms of employees and customers. If the DPIA reveals that the processing poses a high risk that cannot be mitigated by the controller, the National Information Technology Development Agency (NITDA) must be consulted. Thus, organisations are required to assess the impact of the proposed processing on employees, considering its necessity and proportionality, and to identify the risks posed by data processing to personal rights and liberties. Based on this assessment, organisations must then take appropriate measures to mitigate these risks. While the NDPR is silent on the content of the DPIA, the European Union (EU) Article 29 Working Party recommends that all DPIAs be reassessed every three years, or sooner if circumstances change rapidly.[32]

The NDPR contains provisions that mandate employers (as controllers and processors) to implement technical and organisational safeguards to ensure the confidentiality, integrity, and availability of employee data (that is, security measures).[33] The deployment of comprehensive organisational policies and processes – ranging from the configuration of devices in accordance with mobile device policies to the training of employees on procedures for handling incidents such as data breaches, and the adoption of technical measures such as encryption, setting up mobile and cloud firewalls, whitelisting of IP (internet protocol) addresses,[34] installation of intrusion detection systems, anti-virus protections, and malware detection systems – will all aid in the protection of sensitive data on BYODs during remote and hybrid work.

To protect personal data and prevent data breaches caused by the use of BYOD devices, employers should integrate data privacy features and data protection technologies directly into their business practices. These necessary safeguards must be applied to

[30] Section 3.2 (viii) NDPR Implementation Framework.

[31] Section 3.2 (i) NDPR Implementation Framework.

[32] Data Protection Commission (DPC) Ireland (2022b), 'Data Protection Impact Assessments', *@dpcireland*, available at: https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments

[33] Section 2.6 NDPR 2019.

[34] IP whitelisting is a security measure used to restrict access to a computer system or network based on a list of trusted IP addresses. This means that only computers or devices with an approved IP address can access the system, while all other IP addresses are denied access. For example, a company might use IP whitelisting to ensure that only employees on their corporate network can access their internal systems or to allow access only to trusted vendors or partners.

the processing, and any pre-existing configuration value must be adjusted in accordance with the principles of data minimisation and purpose limitation (that is, data protection by design and by default).[35]

2. Nigerian Cybercrime Act

The provisions of the Nigerian Cybercrime Act are relevant to bring your own device (BYOD) policies and practices. The Cybercrimes (Prohibition and Prevention) Act 2015, has a significant impact on cyber law in Nigeria. The Act creates a comprehensive legal, regulatory and institutional framework in Nigeria to prohibit, prevent, detect, prosecute and punish cybercrime.

The Act criminalises unauthorised access to computer systems, including personal devices used for work purposes as part of a BYOD policy.[36] Section 9 of the Act makes it a criminal offence to intercept communications transmitted over a computer system or BYOD devices.[37] Where, however, such interception of electronic communication is carried out pursuant to the order of a judge, because there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of criminal investigation, then such interception is decriminalised.[38] The Nigerian Cybercrime Act further requires that companies report any cybercrime incidents to the Computer Emergency Response Team (CERT) co-ordination, so that it can take necessary measures to tackle the issue.[39] Section 31 of the Act criminalises non-submission of access rights or codes to the employer after disengagement without any lawful reason. A relevant question, in this case, is whether the personal devices of employees used for work purposes fall under the access rights of employers, since they may contain corporate data. It remains to be seen how BYOD issues of this kind will be dealt with in litigation, but employers may put in place clear and comprehensive policies and procedures, providing employees with training and guidance on the use of personal devices for work purposes, and using mobile device management (MDM) software to help secure and manage the devices and data associated with BYOD.

3. Electronic Transactions Act

Section 2 of the Act defines an electronic transaction as any transaction that is created, recorded, processed, stored, retrieved or transmitted by electronic means.[40] This definition includes transactions conducted on personal devices used for work purposes as part of a BYOD policy. Electronic records on BYOD devices are admissible in evidence

[35] Data Protection Commission (DPC) Ireland (2022a), 'Data protection by Design and by Default', *@dpcireland*, available at: https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default

[36] Section 6 Nigerian Cybercrime Act (NCA).

[37] Section 9 NCA.

[38] Section 39 NCA.

[39] Section 21 NCA.

[40] Section 2 Nigerian Electronic Transactions Act (NETA).

in court proceedings, provided that the records are shown to be reliable and trustworthy.[41] Such records are necessarily meant to be made available to the parties who are entitled to access them. Under this Act, electronic signature shall be considered to be as valid as a handwritten signature, provided that the signature is reliable and trustworthy.[42]

The Act, notwithstanding, provides that electronic records be retained for the minimum period necessary, taking into account the type of record, the purpose for which it was generated and the legislation that requires its retention.[43] This includes records stored on personal devices used for work purposes as part of a BYOD policy. Therefore, employers are obliged under this Act to only retain information on personal devices as necessary and in accordance with the law. Under the Nigerian Cybercrime Act, such retention of traffic data shall be for a period of two years.[44]

4. Freedom of Information Act

The provisions of the Freedom of Information Act (FOIA) in Nigeria are relevant to bring your own device (BYOD) policies and practices. The Freedom of Information Act gives everyone the right of access to information, whether in written or electronic form, held by public institutions or officers. The person requesting the information does not need to show any specific interest in the information or justify his/her reasons for making the request.[45] Section 3 of the Act provides for the procedures for making a request for information. However, this request may be rejected on certain grounds, such as international affairs and defence,[46] law enforcement and Investigation,[47] personal Information,[48] trade or commercial secrets,[49] professional circumstances,[50] and for protection of course or research materials.[51] Notwithstanding, an applicant may apply to the court for judicial review within 30 days of rejection of such application.

Public institution employers in Nigeria should be aware of these provisions and should take steps to ensure that they are in compliance with the FOIA when implementing a BYOD policy. This may include putting in place clear and comprehensive policies and procedures, providing employees with training and guidance on the use of personal devices for work purposes, and using mobile device management (MDM) software to help secure and manage the devices and data associated with BYOD. Additionally, employers

[41] Section 7 NETA.
[42] Section 11 NETA; Section 17 of the Nigerian Cybercrime Act (NCA).
[43] Section 10 NETA.
[44] Section 38(1) NCA.
[45] Sections 1 and 2 Freedom of Information Act (FOIA).
[46] Section 11 FOIA.
[47] Section 12 FOIA.
[48] Section 14 FOIA.
[49] Section 15 FOIA.
[50] Section 16 FOIA.
[51] Section 17 FOIA.

should be mindful of the provisions of the FOIA when responding to requests for information and should be prepared to provide access to information in accordance with the provisions of the Act.

Data security issues associated with BYOD in remote and hybrid work

The Nigerian Data Protection Regulation (NDPR)[52] regulates the processing of personal data. All obligations under the NDPR fall on the 'data controller' – typically the employer – who determines the purpose and way data is processed. 'Processing' involves obtaining, storing and utilising data, as well as modifying or erasing it. Employers should not assume that they are the data controller of all information on an employee's personal device merely because the device is used for business purposes. Such an assumption could lead to the employer processing (including erasing) the employee's personal information (as well as the information of the employee's friends and family). Depending on the circumstances, this could constitute a violation of the NDPR and would technically necessitate an assessment of the identity of the data controller in relation to each class of personal data on the device prior to accessing, processing or deleting the data.

In the workplace, BYOD devices will primarily contain two types of data: company data and employee personal data.[53] Company data consist of any sensitive, confidential information about the organisation or its clients. Employers must ensure that employee privacy is protected, so it is essential that company data and employee personal data remain separate and that employers do not have access to employee personal data. Several issues have been identified and analysed against the legal position.

1. Can the employer access personal emails and text messages (SMS), the browsing history, and other data on a personal smartphone or tablet used for work?

Employees may be reluctant to hand over their own devices and allow their employer to review their content, especially if the employer requires access to the device to conduct an investigation into an allegation of misconduct.

As a condition of their participation in the BYOD scheme, employers should consider requiring employees to submit their device and password for periodic inspection. If the employee refuses to co-operate, the employer may discipline (and possibly terminate)

[52] The Nigerian Data Protection Regulation (NDPR) 2019, is the main data protection regulation in Nigeria. Some other laws and regulations that contain provisions on data protection: the 1999 Constitution (as amended); the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 ('the Cybercrimes Act'); the National Identity Management Commission Act 2007 ('the NIMC Act'); the NDPR; the National Cybersecurity Policy and Strategy 2021; the Draft Data Protection Bill 2020 (which is currently going through the legislative process); the Consumer Protection Framework 2016; the Framework and Guidelines for Public Internet Access 2019; Guidelines for the Provision of Internet Service; and the Nigeria Data Protection Regulation 2019: Implementation Framework 2020.

[53] GVZH, 'Data Protection Implications of a Bring Your Own Device Policy', 18 Oct. 2019, https://gvzh.mt/insights/data-protection-implications-bring-your-own-device-policy/ accessed 1 November 2022.

him or her for failing to comply with a reasonable management directive. Whether or not a dismissal under these conditions would be just depends on the facts. If an employer uses an employee's username and password without the proper authorisation to access their personal device, it is extremely unlikely that the employer will process the employee's personal data 'fairly and lawfully', as required by the NDPR.[54] In addition, this would be a violation of the Cybercrimes (Prohibition and Prevention) Act 2015. This is because under the Cybercrimes Act, it is a crime to gain unauthorised access to any computer or its data.[55] A 'computer system' is defined in the Cybercrimes Act as any device or group of interconnected or related devices that process data automatically or interactively.[56] It includes computers, mobile phones and other data-processing devices. The hardware and software device may include input, output and storage components that stand alone or connect to a network or other devices, including computer data storage media. Therefore, if an employer gains unauthorised access to a bring your own device (BYOD), the employer may be subject to a fine.

2. Can employees be compelled to let the company inspect their device when they leave the company, to ensure that all confidential information has been deleted?

Employers may wish to wipe an employee's device upon employment termination or if it is lost or stolen. If the employee's personal data and company data are not separated on the device – for example, by a sandbox – all data on the device will be deleted. If the employee has not recently backed up their personal data, the wipe could result in the employee losing significant, potentially irreplaceable data. Employers should ideally consider using software that separates company data and personal data on the device, as well as requiring employees to consent to the deletion of all data on the device as a condition of their participation in the BYOD programme by including a section on remote wipes.[57] This will serve as a waiver.

The BYOD policy should state that employees may use their own devices to access work data, but that if those devices are stolen or lost, the employer has the authority to remotely wipe them. Any deletion should be limited to company data whenever possible, but policies should seek to exclude liability if an employee's data are lost. The employees

[54] See Section 5(1)(a) of the NDPR, which states that personal data must be collected and processed in accordance with the data subject's consent to a specific, legitimate and lawful purpose. Note that these fairness, specificity, legitimacy and lawfulness requirements are in addition to any other procedures outlined in the regulation or any other instrument.

[55] See Section 6 of the Cybercrimes (Prohibition and Prevention) Act 2015. See also Sections 12, 13, 14 and 16 of the same Act.

[56] See Section 58 of the Cybercrime Act, 2015

[57] On this approach, there are two schools of thought, the first being that every company has the ability to restrict access for employees who bring their own device and, therefore, must sign a written remote work policy. The alternative approach is for a remote work policy to outline what the company expects of remote workers and what the workers can expect from the company.

should be made aware of any onerous requirements of the BYOD policy, such as wiping the device. This may aid in managing employee expectations and reduce the risk of withdrawal of consent.

3. To what extent can the employer monitor and control the smartphone, laptop or tablet?

Remote employees may keep irregular hours and use their devices for both personal and professional purposes, making it nearly impossible for employers to distinguish between monitoring work and private time. Many employers deploy software tools on employee devices to monitor employee activities, such as hidden cameras, data loss protection (DLP) tools, and mobile device monitoring (MDM) tools, to combat this challenge. This software logs keystrokes and tracks mouse movements, which frequently constitutes a violation of employees' right to privacy and the NDPR. A PressReader blog[58] cites a similar case of employee monitoring in which the chief executive officer (CEO) of a furniture store installed four cameras in the store's headquarters to monitor employees without their knowledge and viewed the store's activities via an app while he was in London. This raises questions regarding consent and legitimate interest.

The NDPR[59] recognises consent as a legal basis for processing personal data and includes information on how consent must be obtained and how it can be withdrawn. The NDPR does not recognise a data controller's legitimate interests as legal grounds for processing.[60] Prior to collecting personal data from a data subject, the controller must provide the data subject with information regarding the legitimate interest pursued by the controller or a third party. In addition, the right to erasure and the right to restrict processing apply when there are no overriding legitimate grounds for the processing. In the scenario described in the PressReader blog, this means that the CEO unlawfully processed employee data.

Recent events have demonstrated that excessive employee monitoring and a failure to respect employee privacy are violations of data protection laws. For example, following a recent investigation, the Information and Data Protection Commissioner in Malta fined HSBC 5,000 euros (€) for monitoring an employee's bank.[61] In addition, a Dutch court ordered a Florida-based software development company to pay a former remote employee €75,000 for wrongful termination after he refused to leave the webcam on while he worked. According to the court, the employee's right to privacy was violated

[58] Pressreader, 'Nigerian employers and employee monitoring', 14 June 2021, www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 accessed 1 November 2022.

[59] Section 6 of the Nigerian Data Protection Regulation 2019. In Nigeria, data protection is a constitutional right founded on Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).

[60] Section 6 of the Nigerian Data Protection Regulation 2019.

[61] Times of Malta (2019), 'HSBC fined €5,000 for monitoring employee's bank account', 15 August, available at: https://timesofmalta.com/articles/view/hsbc-fined-5000-for-monitoring-employees-bank-account.728921 (accessed 4 November 2022).

by the instruction to leave the camera on.[62] As a solution, employers could consider requiring employees' consent to monitoring or surveillance activity as a prerequisite for participation in the BYOD programme, with them terminating an employee's network access if consent is withdrawn. However, this will not necessarily comply with the NDPR, as the employee's consent may not have been freely given and is easily revocable.

While there are no specific provisions for the enforcement of workplace privacy in Nigeria, the right is protected by constitutional and statutory provisions. The Constitution of the Federal Republic of Nigeria 1999 (as amended) is a fundamental right that prohibits unreasonable searches and seizures of employees' electronic devices, homes, correspondence, telephone conversations and telegraphic communications. Although the National Industrial Court is also authorised to apply international treaties and covenants, such as International Covenant on Civil and Political Rights, which guarantees the right to privacy, and to consider foreign judgments, it leans toward protecting the human rights of employees in the workplace. The tort of breach of confidentiality and misuse of information are common law remedies to a grievance that an employee may have against his or her employer for the improper use or misuse of his or her personal information.

An employee's right to privacy in the workplace is guaranteed, albeit with limitations. Employers are permitted by law to monitor their employees' internet usage, but they are also required to inform their employees of the monitoring and to not misuse the information obtained. A policy in this regard has therefore proved to be essential, as has its dissemination to the employee.

Analysis of the judiciary's approach to determining cases of BYOD in corporate organisation: a comparative analysis of the BYOD cases in the UK, the US, Canada and Europe with Nigeria

The judiciary's approach to determining cases related to bring your own device (BYOD) varies, depending on the specific legal issues involved and the jurisdiction in which the case is heard. In general, the judiciary tends to approach BYOD cases with a focus on balancing the rights and interests of employees, employers and other stakeholders. The legal system, however, has been slow to address the problems brought on by BYOD policies.[63] In Nigeria, there exists a lack of statutes and case laws addressing BYOD policies. This paper's authors, therefore, aim to draw on the steadily evolving case law in the US, UK, Canada and Europe to illustrate some of the legal issues related to BYOD in corporate organisations. These jurisdictions have growing importance for BYOD-related legal issues in the modern business landscape and the comparative analysis of their approaches can provide valuable insights into best practices and innovative solutions.

[62] NL Times (2022), 'Dutch employee fired by U.S. firm for shutting off webcam awarded €75,000 in court', available at: https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu75000-court

[63] Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 153.

The authors' goal is to understand how local laws and regulations are adapting to these developments and to illustrate the different approaches taken by these legal systems to address the BYOD challenges.

One of the most complex and noticeable issues arising with BYOD policies is when a business is facing litigation (Ibid), especially around e-discovery issues. E-discovery issues can arise in legal proceedings involving bring your own device (BYOD) as personal devices may contain electronically stored information that is relevant to a legal case. In such cases, the process of identifying, collecting and producing relevant electronic information can become complex, costly and present various legal challenges. Such challenges could include: determining what electronic information on personal devices is relevant to the legal proceedings and preserving that information to prevent destruction or alteration of evidence; balancing the right to privacy with the right to discover relevant evidence; collecting and producing electronic information when stored on personal devices that are owned and controlled by employees; and the significant cost of collecting, preserving and producing electronically stored information in BYOD cases where many personal devices are involved. A few cases have been decided across various jurisdictions, laying down some principles on how e-discovery issues in BYOD are handled.

In the case of *Zubulake v UBS Warburg LLC,*[64] the court held that a party was required to preserve electronic information stored on personal devices if it was relevant to the legal proceedings. This case established the standard for reasonable and proportionate discovery of electronic information in the context of civil litigation in the United States. In *O'Grady v Superior Court,*[65] which involved the production of electronic information stored on personal devices in the context of a criminal trial, the court established the principle that personal devices may contain information that is relevant to legal proceedings and may need to be produced as part of the discovery process. In *Jivraj v Hashwani,*[66] the court dealt with the issue of whether a party was required to disclose electronic information stored on personal devices if it was relevant to the legal proceedings. The court held that the party was required to produce the information, but emphasised the importance of balancing the right to privacy with the right to discovery. There was also the case of the warrant to search a certain Apple iPhone cellular telephone,[67] which dealt with the issue of whether the US Government could force Apple to unlock a suspect's personal iPhone in a criminal investigation. The court held that the government's request was reasonable and that Apple was required to assist in the unlocking of the phone.

From the above cases, the courts in various jurisdictions appear to prioritise the importance of the preservation and production of electronically stored information (ESI) on personal devices in legal proceedings. However, the case of *Jivraj v Hashwani* highlights

[64] *Zubulake v UBS Warburg LLC*, 217 FRD 309 (SDNY 2003).

[65] *O'Grady v Superior Court*, 139 Cal.App.4th 1423, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

[66] [2010] EWCA Civ 712, [2010] 2 Lloyd's Rep 534, [2010] IRLR 797, [2010] ICR 1435.

[67] In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, 17-mj-02814 (CD Cal. 2016).

the importance of balancing the right to privacy with the right to discovery. There have not been many specific case laws in Nigeria that address BYOD specifically, but the Federal High Court has jurisdiction to hear cases involving e-discovery and the production of electronic information in the context of civil litigation. While Nigerian law Section 7 of the Electronic Transactions Act provides for the admissibility of electronic evidence in court, copies of ESI have been tendered as evidence in court without any clear protocol for their authentication or admissibility. This was the case in *FRN v Femi Fani Kayode,*[68] where the court rejected a computer print-out in a banker's book as inadmissible. The court opined that this was secondary evidence that was not authenticated and thus inadmissible under the Evidence Act. Thus, it is important for organisations to be aware of the e-discovery rules in Nigeria and to have processes in place to preserve and produce ESI in the event of a legal proceeding. This can include having policies and procedures for the preservation of ESI and the management of electronically stored information, as well as having technology and resources in place to assist with the production of ESI in a legal context.

Lindsey Blair identifies two primary concerns of BYOD policies on e-discovery as accessibility and control.[69] The concept of 'control' refers to the extent to which an organisation can manage and regulate the use of personal devices for work purposes. This includes the ability to access, monitor and secure the data stored on personal devices, as well as the ability to enforce compliance with company policies and regulations (Sophos 2021). A party's duty to deliver to its opponent discoverable information is limited to that information that is within its custody and control.[70] The two relevant questions then are whether an employer is in 'control', since BYOD is not within the immediate control/possession of the employer, and whether an employer's monitoring and management of personal devices used for work purposes is reasonable and in accordance with relevant laws and regulations. Courts have addressed this matter in various ways. For instance, in the case of *Bărbulescu v Romania,*[71] the European Court of Human Rights (ECHR), in determining the balance between employees' and employers' rights, held that an employer's monitoring of an employee's personal communications, even if the monitoring was carried out in accordance with company policy, was a violation of the employee's right to privacy. This decision was similar to that in *R v Cole* (Canada),[72] a case that dealt with the issue of whether the search of an employee's personal laptop by his employer, without a warrant, was reasonable. The court held that the search was unreasonable and violated the employee's privacy rights. Furthermore, in *Ontario (Public Safety and Security) v Criminal Lawyers' Association (Canada),*[73] the court dealt with the

[68] (2019) LPELR-46796(CA).

[69] Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 153.

[70] *Jirak v Abbott Labs., Inc.*, 712 F.3d 351, 360 (7th Cir. 2013).

[71] *Barbulescu v Romania* (61496/08) [2016] I.R.L.R. 235.

[72] *R v Cole*, 2012 SCC 53 (CanLII), [2012] 3 SCR 34.

[73] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23 (CanLII), [2010] 1 SCR 815.

issue of whether an employer's policy of searching personal devices of employees, including those brought from home, was reasonable. Here, the court held that the policy was overbroad and unjustified, and violated the employees' privacy rights.

However, there are cases where the court has held that an employee cannot reasonably expect privacy where specific communications on personal devices are work related. In *Garamukanwa v UK,*[74] the European Court of Human Rights ruled that it was not a breach of the right to privacy when an employer used, during a disciplinary hearing, material found by the police in the employee's notebook and phone, and emails sent to another individual's account. The UK employment tribunal reasoned that since the email was sent to work email addresses and dealt with work matters in part, Mr Garamukanwa could have no reasonable expectation of privacy in relation to the materials used as evidence against him. In Mintz v. Mark Bartelstein & Assoc.,[75] the court dealt with the production of electronic information stored on personal devices used for work purposes and established the principle that employees may have a limited expectation of privacy in information stored on personal devices used for work purposes, subject to certain limitations. Specifically, the court held that any intrusion into an employee's privacy interest must be justified by a significant need, and that the intrusion must be limited to the extent necessary to achieve the legitimate objective. In the case of *City of Ontario v Quon,*[76] the US Ninth Circuit Court of Appeals dealt with the issue of whether an employer's review of an employee's text messages sent on a government-issued pager was a violation of the employee's Fourth Amendment rights. The court held that the employer's review of the text messages was reasonable, given the employer's policy on the use of pagers for work purposes.

The other primary concern is accessibility. 'Accessibility' in the context of bring your own device (BYOD) refers to the ability of employees and other users to access the data and applications they need to perform their work using their personal devices. This can include issues related to compatibility, security and privacy.[77] The relevant questions then are whether an employee is entitled to reimbursement or compensation for expenses related to the use of personal devices for work purposes and whether an employer is liable for damage to personal devices caused by work-related activities.

There have been several cases that have addressed the issue of accessibility. In *Doe v XYZ Corp.*,[78] the question was whether an employer's policy of requiring employees to use their personal devices for work purposes was reasonable. The court held that the policy was reasonable, but emphasised the importance of ensuring that the employees had access to the information and applications they needed to perform their work.

[74] (70573/17) [2019] 6 WLUK 109.

[75] *Mintz v. Mark Bartelstein & Associates, Inc.,* 885 F. Supp. 2d 987 (C.D. Cal. 2012)

[76] Quon, 560 US 746 (2010).

[77] TechTarget, 'BYOD (bring your own device)', (TechTarget, 2023) https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device accessed 24 February 2023.

[78] 887 A.2d 1156 (NJ 2005).

Also, in *King v Canadian National Railway Company (Canada),*[79] the court examined the issue of whether an employee was entitled to compensation for the cost of a personal device that was used for work purposes. The court held that the employee was entitled to be reimbursed for the cost of the device, as well as for other expenses related to accessing and using the data and applications they needed to perform their work. Furthermore, in *Commonwealth Bank of Australia v Barker,*[80] the court dealt with the issue of whether an employee was entitled to be reimbursed for the use of his personal device for work purposes. Here, the court held that the employee was entitled to reasonable compensation for the use of his device.

In *Digital Rights Ireland and Seitlinger et al.,*[81] the Court of Justice of the European Union (CJEU) issued a ruling dealing with the issue of data protection in the context of BYOD. The court held that an employee's personal data processed on a personal device used for work purposes must be protected against unauthorised access and that the employer is responsible for ensuring that appropriate technical and organisational measures are in place to protect these data.

These cases illustrate the challenges and complexities in BYOD cases and demonstrate the need for clear and comprehensive BYOD policies to help address the various legal issues associated with the use of personal devices for work purposes. They also demonstrate the importance of ensuring that employees have access to the information and applications they need to perform their work, regardless of whether they are using personal or company-owned devices. This can include ensuring compatibility with the necessary software and systems, providing necessary security measures, and protecting privacy.

Conclusion

The BYOD culture is advancing rapidly and changing work environments have accelerated this trend. This has exacerbated the data security and data privacy threat landscape. Organisations will need to rethink their data management strategies. This article examines the issues around BYOD ownership and the risks associated with such devices. It also analyses some data protection and security practices associated with BYOD and highlights the role of regulatory bodies in Nigeria in establishing proper compliance standards. The paper further recommends policy interventions to balance the rights and interests of employees, employers and other stakeholders. The article looks at the legal and regulatory framework in Nigeria and the need for organisations to adhere to regulatory standards and self-governing best practices. Very importantly, it evaluates the approach taken by courts in handling cases related to bring your own device (BYOD), drawing from principles established by US, UK, Canadian and European courts and the lessons that can be taken from these by Nigerian courts.

[79] 1922 CanLII 31 (SCC).

[80] [2013] FCAFC 83.

[81] C-293/12 (2014) ECLI:EU:C:2014:238.

References

Books, journals and blogs

Blair, L (2018), 'Contextualizing bring your own device policies', *Journal of Corporation Law*, Vol. 44, 151.

Cavoukian, A (2013) 'BYOD: (Bring Your Own Device) Is Your Organization Ready?' Information and Privacy Commissioner Ontario, Canada, retrieved from https://silo.tips/download/byod-bring-your-own-device-is-your-organization-ready accessed 2 November 2023.

Data Protection Commission (DPC) Ireland, 'Data protection by Design and by Default' available at: www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default accessed 24 Feb. 2023

Data Protection Commission (DPC) Ireland, 'Data Protection Impact Assessments', available at: www.dataprotection.ie/organisations/know-your-obligations/data-protection-impact-assessments

Data Protection Commission (DPC) Ireland, 'Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR', (DPC, October 2019) https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf accessed 4 November 2022.

Guardian Nigeria, 'Ransomware hits 71% of Nigerian Organisations', 4 May 2022, https://guardian.ng/technology/ransomware-hits-71-of-nigerian-organisations/ accessed 4 November 2022.

GVZH, 'Data Protection Implications of a Bring Your Own Device Policy', 18 Oct. 2019, https://gvzh.mt/insights/data-protection-implications-bring-your-own-device-policy/ accessed 1 November 2022.

Imperva, 'Phishing attacks', n.d., https://www.imperva.com/learn/application-security/phishing-attack-scam/ accessed 4 November 2022.

Information Commissioner's Office (ICO), 'Step 5: Identify and assess risks', https://ico.org.uk/for-organisations/childrens-code-hub/sample-data-protection-impact-assessment-online-retail/step-5-identify-and-assess-risks/ accessed 3 November 2022.

Irene, M (2021), 'Nigerian employers and employee monitoring', PressReader, 14 June, available at: www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 (accessed 1 November 2022).

Mantelero, A and G Vaciago (2017), 'Legal Aspects of Information Science, Data Science and Big Data', in M Dehmer and F Emmert-Streib (Eds.), *Frontiers in Data Science,* CRC Press (Boca Raton, Florida).

McLellan ML, Sherer JA, and Fedeles ER (2015), 'Wherever You Go, There You Are (with Your Mobile Device): Privacy Risks and Legal Complexities Associated with International Bring Your Own Device Programs', *Richmond Journal of Law and Technology*, Vol. 21, 1.

NL Times, 'Dutch employee fired by U.S. firm for shutting off webcam awarded €75,000 in court', 9 Oct. 2022, https://nltimes.nl/2022/10/09/dutch-employee-fired-us-firm-shutting-webcam-awarded-eu75000-court accessed 4 November 2022.

Oxford University News Science Blog, 'FBI follows Oxford academics' guide to beat Zoom bombers', 24 April 2020, https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers accessed 24 February 2023.

PortSwigger, 'Remote working during coronavirus pandemic leads to rise in cyber attacks, say security professionals', (PortSwigger, 2020) https://portswigger.net/daily-swig/remote-working-during-coronavirus-pandemic-leads-to-rise-in-cyber-attacks-say-security-professionals accessed 24 February 2023.

Pressreader, 'Nigerian employers and employee monitoring', 14 June 2021, www.pressreader.com/nigeria/business-a-m/20210614/282029035175985 accessed 1 November 2022.

Rai, S, P Chukwuma and R Cozart (2016), *Security and Auditing of Smart Devices: Managing Proliferation of Confidential Data on Corporate and BYOD Devices,* Auerbach Publications (Boca Raton, Florida).

Samsung, 'Maximizing Mobile Value', White Paper, Samsung Business, available at: https://samsung.com/us/business/short-form/maximizing-mobile-value-2022/ accessed 11 September 2022).

Sophos (2021), 'BYOD Security: The Importance of Mobile Device Management (MDM)', retrieved from: www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-byod-security-factsheet-en.pdf

Sophos, 'State of Ransomware in Retail 2022 report', retrieved from https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-retail accessed 4 November 2023.

Technavio, Bring your own device (BYOD) market by end-user and geography - Forecast and analysis 2022-2026 retrieved from https://www.technavio.com/talk-to-us?report=IRTNTR74271&type=sample&rfs=epd&src=report&utm_source=prnewswire&utm_medium=pressrelease+&utm_campaign=t42dtcs_rfs1_wk41_2022_007&utm_content=IRTNTR74271 accessed 1 November 2022.

TechTarget, 'BYOD (bring your own device)', (TechTarget, 2023) https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device accessed 24 February 2023.

Tessian, 'Understand the mistakes that compromise your company's security', retrieved from: www.tessian.com/research/the-psychology-of-human-error/

The Daily Swig (2020), 'Remote working during coronavirus pandemic leads to rise in cyberattacks, say security professionals, 14 July; VMware (2020) *Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat*, available at: https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/ accessed 23 February 2023.

Times of Malta, 'HSBC fined €5,000 for monitoring employee's bank account', 15 August, available at: https://timesofmalta.com/articles/view/hsbc-fined-5000-for-monitoring-employees-bank-account.728921 accessed 4 November 2022.

T-Mobile for Business, The T-Mobile for Business 2020 Workplace Mobility Report, 2020, https://www.t-mobile.com/content/dam/tfb/pdf/T-Mobile-for-Business-2020-Workplace-Mobility-Report.pdf?icid=TFB_TMO_P_TFBFTRWRKS_7LCBNVDVYBXY27WF321599 accessed 1 November 2022.

VMware, Carbon Black Global Threat Report June 2020 – Extended Enterprise under Threat, 2020, https://www.carbonblack.com/resources/global-threat-reportextended-enterprise-under-attack-index/ accessed 4 November 2022.

Wired, 'BYOD, CYOD, COPE, COBO — What Do They Really Mean?', www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/ accessed 2 November 2022.

Yonhap News Agency, 'S. Korea probes cyberattack on digital currency exchange', 3 July 2017, https://en.yna.co.kr/view/AEN20170703010400320 accessed 1 November 2022.

Zippia, '26 surprising BYOD statistics [2022]: BYOD trends in the workplace', Zippia.com, 17 October 2022, https://www.zippia.com/advice/byod-statistics/ accessed 2 November 2022.

Laws, regulations and guidelines

1999 Constitution of the Federal Republic of Nigeria

Credit Reporting Act of 2017.

Cybercrimes (Prohibition and Prevention) Act 2015

European Data Protection Supervisor (EDPS) (2022), 'Guidelines on the protection of personal data in mobile devices used by European institutions (Mobile devices guidelines)', available at: https://edps.europa.eu/sites/default/files/publication/15-12-17_mobile_devices_en.pdf (accessed 2 November 2022).

Freedom of Information Act 2011

NDPR Implementation Framework 2020

Nigerian Data Protection Regulation (NDPR) 2019

Regulation (EU) 2019/881 of the European Parliament and of the EU Council of 17 April 2019 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Further reading

Abdulrauf, LA (2021), 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms', Information and Communications Technology Law, Vol. 30 87–89.

Australian Government (2019), 'Part 3: Responding to data breaches — four key steps', Office of the Australian Information Commissioner, available at: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps

Bispham, M et al. (2021), 'Cybersecurity in Working from Home: An Exploratory Study', available at: SSRN 3897380 (accessed 4 November 2022).

Cavelty, MD (2010), 'Cyber-security', in The Routledge Handbook of New Security Studies, Routledge, p.4.

CyberlinkASP (2014), 'Consider Desktops in the Cloud for BYOD, available at: www.cyberlinkasp.com/insights/consider-desktops-cloud-byod/ (accessed 2 November 2022).

Fruhlinger, J (2022), 'What is Phishing? How This Cyber-attack Works and How to Prevent It', 13 April, CSO, available at: www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-preventit.html (accessed 2 November 2022).

Hakak, S et al. (2020), 'Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies', IEEE Access, Vol. 8, 124134.

Informer, 'A CISO's Guide to Attack Surface Expansion in 2023', (Informer, 12 January 2023) https://informer.io/resources/attack-surface-expansion accessed 24 February,2022.

IT Governance (2022), ‘List of Data Breaches and Cyber Attacks in August 2022 – 97 Million Records Breached’, Itgovernance.co.uk, blog, 1 September, available at: www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached accessed 2 November 2022

KMicro (2019), ‘How to Implement a BYOD Policy Your Employees Will Actually Follow’, available at: https://kmicro.com/how-to-implement-a-byod-policy-employees-will-follow/ accessed 3 November 2022.

Lewis Silkin (no date), Bring Your Own Device, 3, available at: www.lewissilkin.com/api/download/downloadattachment?id=8e57d419-b986-4353-b813-91f6eef3e41e (accessed 2 November 2022).

Mantelero, A et al. (2020), ‘The common EU approach to personal data and cybersecurity regulation’, International Journal of Law and Information Technology, Vol. 28, 297.

Ottis, R and Lorents, P (2010), *‘Cyberspace: Definition and implications’*, Academic Conferences International Limited, available at https://www.proquest.com/docview/869617247/fulltextPDF/17941F23CCD04FBAPQ/1

Veeam (2022a), 2022 Data Protection Trends Report, available at: https://www.veeam.com/wp-data-protection-trends-report.html (accessed 18 September 2022).

Veeam (2022b), ‘Real-World Statistics on Downtime and Data Loss in 2022’, available at: www.veeam.com/blog/data-loss-2022.html (accessed 18 September 2022).

Weil, T and S Murugesan (2020), ‘IT risk and resilience – Cybersecurity response to COVID-19’, IT Professional, Vol. 22, 4.

Commonwealth Cybercrime Journal \ 133
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Cyber Diplomacy Co-operation on Cybercrime between Southeast Asia and Commonwealth Countries: Realities, Responses and Recommendations

Mark Bryan Manantan[1]

Abstract

Amid the onslaught of the COVID-19 pandemic, Southeast Asia's technological innovation footprint has expanded, and its digital economy continues to mature. However, Southeast Asia's vulnerability to cyber threats like cybercrime is also accelerating at a pace commensurate with the region's digital transformation. As geopolitical powerplay colours regional and international co-operation on cybercrime, Southeast Asia's digital prospects will rely on new ways of collaboration. This article examines the growing security implications of cybercrime in Southeast Asia, aiming to formulate effective policy interventions to advance regional and international cyber diplomacy co-operation – through capacity building and multistakeholder partnerships – against the backdrop of the Association of Southeast Asian Nations' (ASEAN's) declining political and institutional power, worsening geostrategic rivalry, and the stalemate of international co-operation on internet governance. It advances the concept of peer-to-peer learning as a practical yet flexible approach to drive cyber diplomacy engagements that will bring key stakeholders together across different jurisdictions. This approach could potentially jumpstart pan-ASEAN co-operation in the short-to-medium term, given the lack or absence of a regional framework on cybercrime.

[1] Director, Cybersecurity and Critical Technologies, Pacific Forum.

The article further explores the peer-to-peer learning model to facilitate cross-regional co-operation among Southeast Asia and Commonwealth countries in Africa, Latin America and the Pacific Island nations. By leveraging a strong network and expertise of law enforcement agencies, regulatory bodies, financial institutions, technology ('tech') companies and civil society organisations located in various jurisdictions through regular exchanges, it becomes plausible to analyse the full scale of cybercrime threats and consequently manage their risks. In effect, developing economies can then prioritise and manage resources effectively to enhance cross-regional cybercrime collaboration, despite the current fragmentation of global internet governance.

Introduction

The COVID-19 pandemic has catalysed Southeast Asia's rapid digital transformation. Since the pandemic, 60 million Southeast Asians have gone online – prompting users to use digital platforms to cope with the disruptions of intermittent lockdowns and the rapid shift to remote working. That meant increased dependence on mobile and cloud services, as well as e-commerce and distance learning.[2] As Southeast Asia eases into the 'new normal', digital adoption is not slowing down. If the trend persists, the region's digital economy could reach approximately US$1 trillion in gross merchandise value by 2030.[3]

Southeast's Asia's prospects in the global digital economy are largely premised on its increasing importance as an emerging online market and its potential to drive innovation through its homegrown tech companies.[4] With more than 887 mobile connections comprising 132 per cent of its total population in 2021, the region is leading in the adoption of mobile connections.[5] With over 400 million users plugged into the internet, digital services such as e-commerce, online media, online banking and finance, health tech, and education tech ('edtech') are expected to continue to thrive.[6] Such a bullish outlook has propped up the region as a lucrative destination of capital investments, recording a deal value of US$11.5 billion in the first half of 2021 alone – one that exceeded

[2] Manantan, MB (2022), 'US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia', *Issues and Insights*, Vol. 22 No. 5, September, available at: https://pacforum.org/publication/issues-insights-vol-22-sr5-us-singapore-advancing-technological-collaboration-and-innovation-in-southeast-asia.

[3] Bain & Company (2021), 'e-Conomy SEA Report 2021: Southeast Asia enters its "digital decade" as the internet economy is expected to reach US$1 trillion in Gross Merchandise Value (GMV) by 2030', 10 November, available at: https://www.bain.com/about/media-center/press-releases/2021/sea-economy-report-2021/.

[4] Manantan, MB (2022), 'US-Singapore: Advancing Technological Collaboration and Innovation in Southeast Asia'.

[5] Neo, K (2021), 'Digital 2021 Southeast Asia Regional Overview', *We are Social*, 8 March, available at: https://wearesocial.com/sg/blog/2021/03/southeast-asia-digital-life-intensified/

[6] Bain & Company (2021),'e-Conomy SEA Report 2021', op. cit. note 3.

2020's cumulative inflow of US$11.6 billion.[7] The increased deal activity and larger valuations have prompted tech companies, especially start-ups, to explore Initial Public Offerings (IPOs) to further raise capital and/or entice investors to monetise their holdings.

The Association of Southeast Asian Nations (ASEAN), a regional bloc comprising ten member states – Indonesia, Malaysia, Singapore, the Philippines, Thailand, Vietnam, Brunei, Cambodia, Myanmar, and Laos – has laid out the foundation of the region's digital economic aspirations under the ASEAN Economic Community blueprint released in 2015.[8] Recognising the unprecedented changes brought by the pandemic, and the urgency of jumpstarting economic recovery, ASEAN published an updated version of its Digital Master Plan 2025. Additionally, the release of the Brunei-led Bandar Seri Begawan Roadmap further cements ASEAN's desire to leverage technology and digital trade to spur economic recovery over the medium-to-longer term.[9]

At the individual country levels, Indonesia, Malaysia, Singapore, Thailand, and Vietnam have released their respective national policy and strategy documents and even roadmaps outlining their vision to seize the opportunities of the emerging data-driven economy. Amid their varying rollout of fifth-generation technology ('5G') and adoption of emerging technologies like artificial intelligence (AI), the region is unequivocally upbeat about riding the momentum of digital transformation.[10] Therefore, the answer to whether the region can withstand the headwinds of its digital transformation journey – due to digital skills shortages and uneven digital infrastructure – is that it will have to.

However, equally concerning to the digital structural challenges that have beset Southeast Asia are the risks and vulnerabilities brought by the rapid digital transformation. As more public and private organisations become interconnected to the 5G network, they are increasingly employing AI-enabled technologies and internet of things (IoT), while migrating to the cloud platform. This integration of digital technologies has expanded the attack surface that malicious cyber actors can exploit. During the pandemic, Naikon – and advanced persistent threat (APT) group – targeted several governments in the Philippines, Vietnam, Thailand, Myanmar and Brunei to gather geopolitical intelligence.[11] Similarly, SharpPanda – a Chinese-linked APT group – also used sophisticated spear phishing emails, a malicious tactic which targets very specific individuals and organizations to obtain classified information. In addition, nefarious actors also installed backdoors to conduct surveillance operations against Southeast Asian governments. Extant cybersecurity

[7] Ibid.

[8] The Internet Society and TRPC Ltd. (2015),'Unleashing the Potential of the Internet for ASEAN Economies', available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_ASEAN_Digital_Economy_Report_Full_s.pdf.

[9] Manantan, MB (2022) 'US-Singapore', op. cit. note 2.

[10] Noor, E and MB Manantan (2022), 'Raising Standards: Data and Artificial Intelligence in Southeast Asia,' *Asia Society Policy Institute*, July, available at: https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf.

[11] *Checkpoint* (2020), 'Naikon APT: Cyber Espionage Reloaded,' *Checkpoint*, 7 May, available at: https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/

literature on Southeast Asia has focused mainly on the strategic implications of state-sponsored APT groups centred on geopolitical flashpoints like the South China Sea.[12] However, the consequential implications of the lack of a regional approach to cybercrime remains underexplored in Southeast Asia. The urgency of adopting more concrete steps that go beyond strengthening cyber hygiene or cyber awareness has received underwhelming attention.[13] This article seeks to fill that gap.

In recent years, cybercrimes that span the spread of malware, ransomware, distributed denial of service attacks (DDoS), data breaches and phishing have seen a dramatic surge in Southeast Asia. Due to increased connectivity, exacerbated by the uncertainty of pandemic lockdowns, cybercriminals have exploited the brewing social anxieties to access, steal and profit from stolen data.[14] With more than 50 per cent of companies based in Singapore falling prey to ransomware in 2021, Singapore's Cybersecurity Agency elevated cybercrime as a legitimate national security risk due to its capacity to cripple networks of large enterprises and, more importantly, compromise the daily operations of small and medium-sized businesses.[15] Despite the obvious threats that cybercriminals pose, ASEAN still needs to adopt a regionwide approach against cybercrime that would facilitate deeper regional co-ordination among law enforcement agencies. The regional bloc's growing list of geopolitical concerns – the South China Sea[16] and Myanmar coup,[17] among others – and the looming pressure to restart the post-pandemic economic recovery are putting major stress on its capacity to demonstrate political and institutional authority. Furthermore, multilateral discussions on a cybercrime treaty have also stalled due to the geopolitical powerplay between the US and China.

[12] Manantan, MB (2020), 'The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea', *Issues & Studies*, Vol. 56 No. 3, available at: https://www.worldscientific.com/doi/10.1142/S1013251120400135; Gomez, MA (2013), 'Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN', *Journal of Communication and Computer,* Vol. 10, available at: https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_Impact_on_ASEAN.

[13] Chang, LYC (2020), 'Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia', *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 6 June, available at: https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_6.

[14] UN Office on Drugs and Crime (UNODC) (2021),'Cybercrime and COVID19 in Southeast Asia: an evolving picture', available at: https://www.unodc.org/documents/Advocacy-Section/UNODC_CYBERCRIME_AND_COVID19_in_Southeast_Asia_-_April_2021_-_UNCLASSIFIED_FINAL_V2.1_16-05-2021_DISSEMINATED.pdf

[15] Low, D (2022), 'Ransomware attacks threaten nations, 137 S'pore firms fell prey in 2021: CSA', *The Straits Times*, 29 August, available at: https://www.straitstimes.com/tech/tech-news/ransomware-attacks-threaten-nations-137-spore-firms-fell-prey-in-2021-csa.

[16] Manantan, M (2019), 'The Cyber Dimension of the South China Sea Clashes', *The Diplomat*, 5 August 2019, available at: https://www.philstar.com/headlines/2022/12/21/2232369/philippines-concerned-over-report-chinas-construction-activities-spratlys

[17] Editorial Board ANU (2023), 'Myanmar presents ASEAN with only bad options', *East Asia Forum*, 16 January 2023, available at https://www.eastasiaforum.org/2023/01/16/myanmar-presents-asean-with-only-bad-options/

This article will examine the growing security implications of cybercrime in Southeast Asia in order to suggest effective policy interventions to advance regional and international cyber diplomacy co-operation against the backdrop of ASEAN's declining political and institutional power, worsening geostrategic rivalry, and the stalemate of co-operation on internet governance at the global level. Defined as the use of diplomatic tools and initiatives to achieve a state's national interest in cyberspace – mainly through the provision of cyber capacity-building and confidence-building measures, and the development of norms – 'cyber diplomacy' allows the exchange of technical and policy know-how to build resilience against cybercrime.[18] Although Southeast Asia has become an active player in cyber diplomacy itself, the disruptive nature of emerging technologies and the shifting modus operandi of state-sponsored hackers and cybercrime groups have left the region scrambling for effective and agile solutions.

Given the situation, this article seeks to explore other avenues that defy the conventional dyad of co-operation between ASEAN and its existing dialogue partners like the US, Japan, Australia, China, South Korea etc. The article argues that countries in Southeast Asia could adopt a peer-to-peer learning approach to cyber diplomacy engagements beyond the 'usual suspects'. This means engaging other key stakeholders from various sectors across different jurisdictions, such as those located in Africa, Latin America, or Pacific Island nations. The proposed peer-to-peer learning approach could potentially catalyse fresh and innovative analysis to fortify regional co-operation against the risks and vulnerabilities of cybercrime in the short-to-medium term.

This article defines a peer-to-peer learning approach based on a collaborative partnership that involves developing economies, mainly via Global South-to-South dynamics, and goes beyond the conventional developed–developing country relationships.[19] Through the adoption of peer-to-peer learning among the technologically advanced countries in Southeast Asia – comprising of Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam – the article will offer key insights that can strengthen ASEAN's declining decision-making processes in the face of urgent and rising threats like cybercrime. In exploring the peer-to-peer learning approach, the article aims to further enrich the cyber diplomacy literature, specifically the cyber capacity-building portfolio in Southeast Asia that has often been dominated by literature on donor–recipient relations, primarily from ASEAN's dialogue partners like Japan and Australia.[20] The article also contends that the peer-to-peer learning model could help facilitate deeper co-operation among Southeast Asia and Commonwealth countries in Africa, Latin America and the Pacific Island nations. With shared interests towards maintaining an inclusive, neutral and multilateral

[18] Manantan, MBF (2021), 'Advancing cyber diplomacy in the Asia Pacific: Japan and Australia', *Australian Journal of International Affairs,* available at: https://www.tandfonline.com/doi/full/10.1080/10357718.2021.1926423.

[19] Collett, R (2021), 'Understanding cybersecurity capacity building and its relationship to norms and confidence-building measures', *Journal of Cyber Policy* , available at: https://www-tandfonline-com.ezproxy.lib.rmit.edu.au/doi/full/10.1080/23738871.2021.1948582?src=recsys.

[20] Manantan, MBF (2021) 'Advancing cyber diplomacy in the Asia Pacific', op. cit. note 15.

platform, small and medium power countries can bond together to co-ordinate on a narrow and well-defined set of functional areas of co-operation, such as cybercrime, that demonstrate their agency and autonomy. Due to the intense competition brought by the US and China, the concept of peer-to-peer learning serves as an attractive and viable model for a co-operative framework. It could jumpstart cross-regional co-operation among countries in Southeast Asia, South Asia, Africa, Latin America and the Pacific amid the uncertainty of achieving international consensus on cybercrime co-operation in the foreseeable future.

The article expands on its main argument in three stages. First, it will conduct a brief examination on the underlying *realities* of technologically capable countries in Southeast Asia against the growing threats of cybercrime. From there, it will examine the *responses* undertaken at the regional level through ASEAN and at the individual country level. This section will highlight various avenues through which Southeast Asia is 'bridging the gap' in terms of internal and external capacity-building co-operative mechanisms. After this assessment, the paper will offer policy *recommendations* on how Southeast Asia can play a more proactive role in cyber diplomacy in tackling cybercrime through peer-to-peer learning within the region, as well as exploring collaboration with Commonwealth countries in Africa, Latin America and the Pacific Islands nations.

Realities: setting the cybercrime landscape

Due to increasing digital connectivity and compounded by the social anxieties from the pandemic, Southeast Asia has become a fertile ground for cybercriminals to test and launch their illicit activities. More importantly, the region's weak and/or absent legislative and policy frameworks for investigating and prosecuting cyber-related crimes make it the ideal operational environment for cybercriminals and syndicates to conduct and continuously refine their operations. This section provides an overview of the cybercrime landscape in Southeast Asia, highlighting (1) prevailing cybersecurity threats, trends and tactics employed by malicious actors; (2) rising incidents of ransomware and exploitation of cryptocurrency; and (3) an absence of cybercrime policies and legislative gaps.

Prevailing cybersecurity threats, trends, and tactics

The Asia Pacific region, particularly Southeast Asia, has higher-than-average rates of malware and ransomware attacks. Microsoft found that the region has rates 1.6 or 1.7 times higher than the global average.[21] Through a concerted and collaborative partnership with key stakeholders from the public and the private sectors, Interpol's *ASEAN Cyberthreat Assessment 2021* report identified the following as the top cybercrime threats: (1) business e-mail compromise (BEC); (2) phishing; (3) ransomware;

[21] Microsoft Stories Asia (2022), 'Microsoft launches first Asia Pacific Public Sector Cyber Security Executive Council across seven markets in the region', 31 May, available at: https://news.microsoft.com/apac/2021/05/31/microsoft-launches-first-asia-pacific-public-sector-cyber-security-executive-council-across-seven-markets-in-the-region/.

(4) e-commerce data interception; (5) crimeware-as-a-service; and (6) cyber fraud. Interpol ranked ransomware as the most significant threat in Southeast Asia, one that is proliferating at an unprecedented rate because barriers to entry are low, and it is affordable to execute. In addition, ransomware-as-a-service (RaaS), crimeware-as-a-service (CaaS) and phishing-as-a-service (PhaaS) are also becoming popular for making a quick profit. These are business models between ransomware operators and affiliates. In this set-up, affiliates, who do not have the skillset to develop ransomware, pay operators to launch ransomware attacks. Put simply, RaaS, CaaS, and PhaaS operate in a similar fashion to the software as a service (SaaS) business model.[22] Interpol also emphasised the increasing propensity among cybercriminals to exploit the growing ubiquity of IoT devices, using various tactics to obtain maximum illicit gains. The report also noted that open-source information is vital to crafting effective social engineering scam tactics against individuals and organisations.[23] Furthermore, with the e-commerce boom, cybercriminals are deploying an increasing number of JavaScript card sniffers to siphon proprietary financial and personal information.

Rise in ransomware incidents and exploitation of cryptocurrency

Microsoft's Digital Crimes Unit made parallel observations, noting the low-cost yet high-profit yield of ransomware as a cybercriminal activity. Meanwhile, well-resourced cybercriminals who can operate at larger scales have deployed armies of infected computers to launch simultaneous malware attacks. Other cybercriminals have adopted a 'mix and match strategy'; for instance, BEC have used sophisticated phishing attacks to lure victims, steal information and redirect money to criminal bank accounts, while tech-support scams have been quite effective, especially amid the looming financial distress that took place at the height of the COVID-19 pandemic.[24]

Based on a survey of more than 900 IT executives and professionals, Kaspersky found that 67 per cent of businesses in Southeast Asia had become victims of cybercrime in 2020. Most of the victims (82.1%) confessed to having paid the ransom demand – higher than the global average of 38.1 per cent.[25] Kaspersky also reported that 47.8 per cent of the victims paid the ransom as soon as possible to mitigate any disruption to business operations, while 23.9 per cent attempted to recover data through backup or decryption before giving in and having to pay within two days. Only a small percentage, 10.4 per cent,

[22] Baker, K, 'Ransomware as a Service (RAAS) Explained How It Works & Examples', *Crowdstrike*, January 30, 2023, available at https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

[23] Interpol (2021), *ASEAN Cyberthreat Assessment 2021*, available at: https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf.

[24] Manantan, MB and D Mitchum (2021), 'Key Findings Adapting to COVID-19 Indonesia, the United States, and the Indo-Pacific', Session #2 Assessing Cybersecurity Trends and Threats in the US and Indonesia, Pacific Forum, 29 March, available at: https://pacforum.org/wp-content/uploads/2021/03/210329_US-Indonesia_KeyFindings.pdf.

[25] Zulhusni, M (2022), '67% of businesses in SEA found themselves as victims of ransomware attacks', *Techwire Asia*, 17 August, available at: https://techwireasia.com/2022/08/67-of-businesses-in-sea-found-themselves-as-victims-of-ransomware-attacks/.

resisted for a week and eventually paid the demand ransom. According to the *Unit 42 Ransomware Threat Report 2021*, the average ransom demand has increased up to 144 per cent, citing an 85 per cent surge in the number of victims whose names and details were posted on the dark web's leak sites. The hack and leak modus operandi of cybercriminals is proving to be one of the most evolving coercive tactics among cybercriminal groups, the aim being to increase the pressure on their victims with the ultimate end goal of demanding a higher ransom.[26]

Conducting a deeper analysis on the increasing role of the dark net in facilitating cybercrime in the region, the United Nations Office on Drugs and Crime (UNODC) confirmed the alarming rise in dark net cybercrime in Southeast Asia.[27] The dark web has become a major platform for people to engage in illicit activities, from buying and selling cybercrime toolkits, acquiring stolen credit card details and personal identifiable information from breaches, to trading online child sexual exploitation material.[28] Cryptocurrencies are the primary payment method on dark nets, while Bitcoin is the primary tool to exchange crypto to fiat (that is, the currency issued by countries).

Southeast Asia's proximity to key cyber actors like North Korea make it both a target and an accomplice in cybercrime. In 2019, the UN Security Council's Sanctions Committee on North Korea revealed how Pyongyang's cyber activities stole billions of dollars from financial institutions and cryptocurrency exchanges to generate income.[29] Lazarus, a North Korean cyber-hacking group, was the culprit behind the highly publicised Bangladesh Central Bank heist in 2016 that diverted funds to the Philippines, Sri Lanka and other parts of Asia.[30] A North Korean cyber expert contends that Pyongyang relies heavily on foreign affiliates based in Southeast Asia to convert stolen cryptocurrency funds into fiat. Established links with over-the-counter brokers in foreign countries enable North Korean cybercriminals with money-laundering capacity to finance Kim Jong-Un's regime to develop intercontinental ballistic missiles.[31]

[26] Unit 42 (2022), *2022 Unit 42 Ransomware Threat Report*, Unit 42 – Paloalto Networks, available at: https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.

[27] UNODC (2022),'Darknet Cybercrime Threats to Southeast Asia', available at: https://www.unodc.org/documents/southeastasiaandpacific/darknet/index.html.

[28] Ibid.

[29] Seibt, S (2019), 'How cybercrime funds North Korea's nuclear programme', *France 24*, 8 August, available at: https://www.france24.com/en/20190808-cybercrime-north-korea-nuclear-programme-hacking-china-ballistic-missile.

[30] Zetter, K (2016), 'That Insane, $81M Bangladesh Bank Heist? Here's What We Know', *Wired*, 17 May, available at: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know.

[31] Interview with South Korean cybersecurity experts.

Terrorism and violent extremism remain imminent threats in Southeast Asia. Like other malicious actors, they are also adapting to the online environment. Cryptocurrencies offer means for illicit funds transfer, while ransomware and malware can support their strategic operations. This opens the possibility for violent extremist groups to engage with cybercriminals for weapons-related transactions.[32]

Absence of cybercrime policies and legislative gaps

UNODC contends that Southeast Asia's policy and legal gaps permit cybercriminals to evade detection from law enforcement agencies. The lack of legislative framework provides cybercriminals with a myriad of opportunities to constantly reinvent their business and operational models to maximise profit from virtual-based illicit financial flows and money laundering.[33] Although cybercrime is considered an international or transnational phenomenon, its local dimension should be equally factored into the equation. Experts interviewed in this study asserted that because of the lack or absence of policies and legislative frameworks, law enforcement agencies were prevented from increasing information sharing, conducting comprehensive investigations and facilitating cross-border co-operation.

The perceived deficiency of Southeast Asia's cybercrime legislation, combined with these debilitating technical and policy capacity gaps, make the region a safe harbour for cybercriminals. Vietnam and Malaysia stand out as the region's emerging cybercrime hubs, capturing the global–local dynamics of such illicit activity. Vietnam has a growing 'black hat' (criminal) community, supported in part by the country's strong emphasis on computing and STEM (science, technology, engineering, mathematics) disciplines. Aside from malware and fraud, most hackers are trained on intrusions to conduct data theft, BEM and financial fraud.[34] Although cybercrime and hacking are not synonymous in cybersecurity parlance, in Vietnam, cybercrime is closely linked to hacking. Prevailing corruption in the country also hampers the prosecution of cyber offenders under the full extent of the law. In the case of Malaysia, cybercriminals are not only found among the local population, but also among foreign offenders relocated to the country, most notably from Nigeria. Nigerian cybercriminals have a 'wide footprint' operating beyond West Africa, including in the US, the UK, the Netherlands, India, the Philippines and Australia. For a time, Malaysia hosted the largest number of 'expat' Nigerian fraudsters. Although the cybercrime activities in these cases are relatively low-tech scams such as BEM, the

[32] Franco, J (2021), 'CENS Expert Survey on Extremism Report: Current and Emerging Threats', *RSIS*, July, available at: https://www.rsis.edu.sg/wp-content/uploads/2021/07/PR_CENSExpertSurveyOnExtremismReport_D2.pdf.

[33] Ibid.

[34] Lusthaus, J (2020), 'Cybercrime in Southeast Asia', *Australian Strategic Policy Institute*, available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-05/Cybercrime%20in%20Southeast%20Asia.pdf.

impacts are still damaging. Nigerian cybercriminals capitalise on local social connections to adapt and learn the local language and culture and, soon, establish possible collaborators to enhance their operations.[35]

Responses: confronting the growing threats of cybercrime

Southeast Asia's collective response to the threats of cybercrime has relied on both internal and external mechanisms designed to bolster capacity and co-ordination at the legal, policy and technical levels. This section examines the opportunities and challenges that would permit and inhibit efforts to counter cybercrime in the region, as well as prospects for peer-to-peer learning.

Opportunities

Provision of cybersecurity strategies and initiatives

Building on the ASEAN Cybersecurity Cooperation Strategy (2017–2020), ASEAN has released the Cybersecurity Cooperation Strategy 2021–2025 to outline the establishment of the ASEAN Cybersecurity Coordinating Committee, which embeds cross-sectoral collaboration on cyber issues.[36] It also established the ASEAN Ministerial Conference on Cybersecurity to tackle the growing threats of ransomware at the first substantive session of the Open-Ended Working Group on the Security of and in the Use of ICTs.[37] ASEAN has established robust cybersecurity co-operation among its key dialogue partners and other international organisations, such to improve information sharing on threats and incident response.[38] As a form of confidence building measure, the ASEAN Regional Forum developed a Points of Contact Directory for preventive diplomacy. The directory seeks to reduce the risk that misunderstanding and misperception of information and communication technology (ICT) security incidents, may lead to miscalculation and escalation if left unaddressed.[39]

[35] Ibid.

[36] ASEAN (2022), 'ASEAN Cybersecurity Cooperation Strategy', 26 November, available at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

[37] ASEAN (2021), 'Statement on Behalf of the Association of Southeast Asian Nations', 13 December, available at: https://documents.unoda.org/wp-content/uploads/2021/12/ASEAN-Statement-OEWG-First-Substantive-131221.pdf.

[38] ASEAN (2022), 'ASEAN Cybersecurity Cooperation Strategy,' op. cit note 32.

[39] ASEAN (2019), 'ASEAN Regional Forum (ARF) Points of Contact Directory on Security of and in the Use of Information and Communications Technologies (ICTs)', ASEAN Regional Forum, March, available at: https://aseanregionalforum.asean.org/wp-content/uploads/2019/06/ANNEX-4-Comments-on-CBM1-Final-Concept-Paper-24-May-Clean.pdf.

Co-operation with multilateral bodies and institutions

On cybercrime, UNODC and Interpol have played active roles beyond awareness raising to initiate cross-border collaboration, especially among law enforcement officers, prosecutors and cybercrime inspectors. UNODC has conducted several exercises on digital forensics to strengthen national and cross-border operational capacity. Its ongoing research and capacity-building efforts are also filling the data gap regarding dark web criminality in the context of cybercrime in Southeast Asia. Through its Financial Action Task Force (FATF), UNODC is also working closely with the financial and business sector to identify chokepoints for cryptocurrencies and related money laundering services used by cybercriminals and syndicates in Southeast Asia.[40] In partnership with cybersecurity firms, Interpol has also launched various initiatives to prosecute and investigate cybercriminals that operate as part of a global crime network in the Asia Pacific. In March 2020, it established the ASEAN Cybercrime Operations Desk to enhance cybercrime intelligence and co-ordinate several multijurisdictional operations to target cybercrime.

Challenges

Diverging perceptions on ransomware

Despite the growing list of accomplishments that demonstrates Southeast Asia's agency to proactively arrest the evolving nature of cybercrime, several challenges are still on the horizon that may hamper a holistic and collective regional response. First, the region still operates on a dichotomy that tends to view ransomware through a narrow window. Debates on how to treat cybercrime – whether as a local or global phenomenon or whether it occurs purely online – are still prevalent. The Global Forum on Cyber Expertise (GFCE) argues that some governments in the region still do not consider cybercrime to be a threat.[41] This perspective is widely adopted in Southeast Asia, where the marked disparity on digital maturity among member states plus the differing views surrounding cybersecurity as a national security issue downgrade its prioritisation in actual policy implementation.[42] For instance, the cyber dimension of the South China Sea issue[43] – which often manifests through large-scale cyberespionage and/or cyber coercion – is still

[40] UNODC (2022), 'Darknet Cybercrime Threats to Southeast Asia', op. cit. note 23.

[41] Walsh, N (2017), 'UNODC: Countering cybercrime in Southeast Asia and beyond', *GFCE*, 21 November 21, available at: https://thegfce.org/unodc-countering-cybercrime-in-southeast-asia-and-beyond/.

[42] Heinl, C (2014), 'Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime', *Asia Policy*, Vol. 18, available at: https://www.jstor.org/stable/24905282.

[43] Manantan, MB (2020), 'The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea', *Issues & Studies*, Vol. 56 No. 3, available at: https://www.worldscientific.com/doi/10.1142/S1013251120400135; Gomez, MA (2013), 'Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN', *Journal of Communication and Computer*, Vol. 10, available at: https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_Impact_on_ASEAN.

considered an 'isolated issue' and has not reached the level of national security risk.[44] Of course, doubts over ASEAN's ability to genuinely deliver its commitment on cybersecurity also looms given its diminishing credibility to demonstrate political unity.

The lack of a region-wide cybercrime framework

Second, the adoption of a region-wide cybercrime framework in the region remains elusive, in large part due to contentious political issues on the application of sovereignty in cyberspace. Aside from the Philippines, most ASEAN member states have not acceded to the Budapest Convention, an international treaty that tackles crimes committed through the internet and other computer networks.[45,46] Regionally, there is a general sense that the Budapest Convention is highly 'Western centric', owing to its roots in the European Convention on Human Rights. Each country in Southeast Asia has varying perceptions on human rights and tends to prioritise state sovereignty and non-interference. As such, codifying the treaty via domestic legislation remains a mere aspiration.[47] Despite ASEAN's adoption of the Declaration to Prevent and Combat Cybercrime, it remains to be seen if this could lead towards it crafting a regional cybercrime framework akin to the Budapest Convention under its difficult, and often painfully slow, consensus decision-making process.[48]

The lack of a streamlined regional approach on cybercrime thus presents profound implications for building cyber resilience at the strategic and operational levels. This impacts Southeast Asia's capacity to streamline efforts on information sharing and identify common grounds to enforce rules against cybercrime. To their credit, most ASEAN member states have adopted cybercrime legislation on fraud and forgery, and online child pornography; however, there remains a huge disparity in defining the conduct of criminal activities in cyberspace.[49] These disparate approaches affect ASEAN member states' ability to better co-ordinate the collection of real-time data and retain electronic evidence. In effect, law enforcement agencies face bureaucratic and legal hurdles in facilitating the preservation of stored computer data and disclosure of preserved traffic data. Additionally, establishing mutual assistance to access network servers and data

[44] Interview with foreign policy experts in the Philippines.

[45] Council of Europe (2022), 'Details of Treaty No. 185', 26 November, available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

[46] Benincasa, E (2021), 'ASEAN needs to enhance cross-border cooperation on cybercrime', *The Strategist*, 19 January, available at: https://www.aspistrategist.org.au/asean-needs-to-enhance-cross-border-cooperation-on-cybercrime/.

[47] Chen, Q (2017), 'Time for ASEAN to Get Serious About Cyber Crime', *The Diplomat*, 2 August, available at: https://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/.

[48] Kono, K (2022), 'ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone', *CCDOE*, 26 November, available at: https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/.

[49] Chang, LYC (2020), 'Legislative Frameworks Against Cybercrime', op. cit. note 12.

and seeking consent where possible are also impeded.[50] These realities continue to stifle genuine progress in advancing cross-border legal assistance across the region, while such assistance lies at the heart of addressing transnational threats like cybercrime.

Diverging definitions of cybercrime

Even at the multilateral level, Southeast Asian countries have yet to reach a unified position, as clearly shown during the recent deliberations at the UN to establish an international cybercrime treaty.[51] While most Western countries argue that the current Budapest Convention is working and flexible enough to adopt modifications, with the addition of protocols reflecting recent changes in the ICT landscape, Russia and China are dissatisfied with the current cybercrime treaty. Both assert that the convention's emphasis on transborder access to data and electronic evidence could impinge on national sovereignty – a perspective shared across Southeast Asia. The obvious mistrust within both camps – developing and developed economies – also colours the motivation of the ongoing negotiation, which manifests at the most fundamental level: defining cybercrime. As it stands, there is a general agreement on cyber-dependent crimes like malware and ransomware; however, there is no consensus on cyber-enabled crimes, which involve offenses that employ technology to achieve one's strategic or financial ends.[52] What makes the current rounds of deliberation even more problematic is the demand among other states, especially among developing economies, to go beyond cyber-dependent crimes. That means the inclusion of certain provisions to tackle content-related activities that may result in criminalising personal communications, online political speech, and freedom of expression and association. Among ASEAN member states, Indonesia has been the most vocal, alongside Russia and China, on including provisions on issues such as the incitement of terrorism, disinformation and hate speech.

Several civil society organisations are quick to point out that broadening the scope of the proposed treaty may inflict serious damage on fundamental human rights, particularly the freedom of expression.[53] Based on existing studies, cybercrime laws that are vaguely worded or framed in overly-broad terms have been routinely misused by governments to target dissenters.[54] Stepping into the debate, the UN Office of the High Commissioner for Human Rights (OHCHR) stressed that the inclusion of content-related offenses has been

[50] Benincasa, E (2021), 'ASEAN needs to enhance cross-border cooperation on cybercrime', op. cit. note 41.

[51] Walker, S (2022), 'The Quixotic Quest to Tackle Global Cybercrime', *Foreign Policy*, 11 February, available at: https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/.

[52] Walker, S (2022), 'The Quixotic Quest to Tackle Global Cybercrime', *Foreign Policy*,

[53] Brown, D (2022), 'Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks', *Human Rights Watch*, 28 April, available at: https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks.

[54] Human Rights Watch (2021), 'Abuse of Cybercrime Measures Taints UN Talks', 5 May, available at: https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

problematic for human rights, and should not be included in the proposed treaty.[55] The frictions underpinning the first session on the proposed cybercrime treaty resulted in a no consensus text on the objectives and scope, leaving it open. The current political gridlock on addressing cybercrime at the regional and multilateral levels presents a clear and present danger for citizens, organisations, and institutions within and beyond Southeast Asia.

Although Southeast Asia aims to maintain its neutral diplomatic stance to avoid a 'winner takes all' attitude, the current geostrategic climate is becoming untenable for its continuing desire for agency and autonomy. The diplomatic space for policy manoeuvring is shrinking due to the geopolitical competition between the US and China and the spill-over effects of Russia's unprovoked invasion of Ukraine. Mindful of these systemic risks, Southeast Asia should explore a level-headed, yet flexible, response. Hope lies on the continuing interest among states to increase technical capacity. In the short-to-medium term, training assistance will continue to bridge international co-operation. Overtime, these interventions may influence the preference, and even willingness, of countries to close the gap on the scope, intent, and purpose of a region-wide cybercrime framework in Southeast Asia.

Prospects for peer-to-peer learning

In managing the fragmentation of regional and even global co-operation, Southeast Asia could lean towards collaborating beyond its usual partners and explore other types of co-operation among similar and like-minded states who share the same experiences and interests of advancing equitable solutions to cybercrime. Technologically advanced countries like Singapore have demonstrated a strong interest towards leading cyber diplomacy efforts within and beyond the region framed around the peer-to-peer learning approach. The city-state has had its fair share of high-profile data breaches and ransomware incidents,[56] but its track record on addressing the significant gaps in cyber capacity building at the technical, policy and operational levels presents an interesting case study on peer-to-peer learning to tackle cyber-related threats like cybercrime.

Singapore tabled the formation of a working group on cybercrime during the 13th ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) in 2013. Since then, the Cybercrime Working Group has conducted relevant trainings to improve information sharing and facilitate the exchange of best practices, techniques and tools. It has also sought to engage stakeholders from law enforcement and the private sector to establish strategic partnerships.[57] In response to the sudden spike of cybercrime during the

[55] UN Human Rights Office of the High Commissioner (2022), 'OHCHR key messages relating to a possible comprehensive International Convention on countering the use of Information and Communications Technologies for criminal purposes', OHCHR, 17 January, available at: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf.

[56] Low, D (2021), 'Ransomware attacks threaten nations', op. cit. note 14.

[57] ASEAN (2014), 'ASEAN Working Group on Cybercrime,' 27 May, available at: https://asean.org/wp-content/uploads/2021/01/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf.

pandemic, Singapore organised the Fourth ASEAN Plus Three Cybercrime Conference in 2021. As the designated ASEAN Lead Shepherd for cybercrime, Singapore held a workshop to share best practices and upgrade the competencies of law enforcement officers in the region. It also hosted the Eighth Senior Officials Roundtable on Cybercrime, which discussed new initiatives among industry partners.[58]

Outside of Southeast Asia, Singapore's engagement to improve Ghana's cybersecurity offers insights on the potential of peer-to-peer learning in cyber capacity building. During Singapore International Cyber Week 2022, Ghana's minister for communications and digitalisation revealed that she had held bilateral discussions with Singapore's minister for communications and information. The current bilateral cybersecurity co-operation focuses on critical information Infrastructure protection, regulation of cybersecurity service providers, as well as professional exchanges between officials of the Cybersecurity Agency of Singapore and the Cybersecurity Authority of Ghana. Singapore's Cyber Security Agency has been actively exchanging best practices with Ghana's Cyber Security Authority to improve its National Computer Emergency Response Team and institutionalise a multi-stakeholder approach within the Joint Cybersecurity Committee and the Industry Forum, which were established under Ghana's Cybersecurity Act 2020.

Beyond bilateral engagements, the two countries are also collaborating at the international level. Singapore has acknowledged Ghana's election to the International Telecommunications Union (ITU) Council and its support to its UN-Singapore Cyber Fellowship. Likewise, Singapore's top cybersecurity officials have also participated in Ghana's National Cybersecurity Awareness Month. Singapore and Ghana also affirmed the importance of collaborating with Interpol's Global Complex for Innovation, which is its technology branch, dedicated to improving global cybercrime response through legal assistance and digital forensics capabilities.[59]

On law enforcement, Malaysia has been actively co-operating with Interpol authorities, given the serious impact of alleged Nigerian fraudsters in the country. In October 2022, Malaysia participated in Operation Jackal, a joint law enforcement effort which targeted an international cybercrime ring known as Black Axe.[60] This West African organised crime group has been responsible for massive cyber-enabled financial crimes worldwide. In operationalising Operation Jackal, Interpol worked with law enforcement agencies to

[58] ASEAN (2022), '16th ASEAN Ministerial Meeting on Transnational Crime (AMMTC) Plenary-Country Statement by Associate Professor Dr Muhammad Faishal Ibrahim, Minister of State, Ministry of Home Affairs and Ministry of National Development', Ministry of Home Affairs, 21 September, available at: https://www.mha.gov.sg/mediaroom/speeches/16th-asean-ministerial-meeting-on-transnational-crime-ammtc-plenary-country-statement.

[59] Citi Newsroom (2022), 'Ghana holds bilateral meetings with Singapore to improve its Cyber security development', 25 October, available at: https://citinewsroom.com/2022/10/ghana-holds-bilateral-meetings-with-singapore-to-improve-its-cyber-security-development.

[60] Interpol (2022), 'International crackdown on West-African financial crime rings', 14 October, available at: https://www.interpol.int/en/News-and-Events/News/2022/International-crackdown-on-West-African-financial-crime-rings.

deploy the Anti-Money Laundering Rapid Response Protocol (ARRP), a global stop-payment mechanism which has helped in the investigation of suspects and identification of assets.[61] In close co-ordination with Interpol's Global Financial Crime Task Force, the ARRP enabled the joint law enforcement operations to intercept illegal proceeds of crime. Malaysia's participation in Operation Jackal was crucial, given the increasing number of cybercrime-related activities of alleged Nigerian fraudsters in the country. Since 2014, US and UK authorities have also tracked down reports of malicious internet scams involving Nigerian racketeers operating in Malaysia that utilise online dating sites.[62]

Recommendations: advocating for a peer-to-peer learning approach to cybercrime

The deepening 'zero-sum game' in the current geostrategic environment makes the idea of peer-to-peer learning among small-to-medium sized states an alternative and viable mode of cyber diplomacy co-operation, especially in the interconnected world of tech. With little chance of governments coming together to compromise amid competing interests, agreeing an international cybercrime treaty remains uncertain in the foreseeable future. Countries that feel excluded from the decision-making process could band together to work on a narrow and well-defined set of functional areas of co-operation to demonstrate their agency and autonomy.

The possible cross-regional co-operation among Southeast Asia and Commonwealth countries in South Asia, Africa, Latin America and the Pacific could be a starting point to continue the discussions on cybercrime. However, co-operation across these jurisdictions will still require significant investments. Undeniably, developing economies often rely on external partners to augment resource constraints. To supplement possible resource shortages, a network of experts and practitioners specialising in cybersecurity based in think tanks, research universities and private companies could catalyse cross-border co-operation. Built around the fundamental tenets of cyber diplomacy, the following recommendations are provided to bolster Southeast Asia's collective cybercrime engagement efforts, driven by a peer-to-peer learning approach within and beyond the region.

Internal peer-to-peer learning among ASEAN member states

The first recommendation is the establishment of a cybercrime 'minilateral' grouping. The ASEAN minus X model – where some member states could opt out from the decision-making process – has become the sought-after remedy to ASEAN's declining

[61] Arghire, I (2022), '75 Arrested in Crackdown on West-African Cybercrime Gangs', *Security Week*, 17 October, available at: https://www.securityweek.com/75-arrested-crackdown-west-african-cybercrime-gangs.

[62] Campbell, C (2014), 'Malaysia is Becoming a Global Hub for Internet Scams Preying on the Lovelorn', 9 July, available at: https://time.com/2968765/malaysia-is-becoming-a-global-hub-for-internet-scams-preying-on-the-lovelorn.

consensus-building approach. Although in *theory* the model presents a feasible solution to the regional bloc's slow and ineffective decision-making process, its *practical* application in the field of cybersecurity would still require overcoming political sensitivities and security considerations within the group. For instance, the drawbacks of potential retaliation – through military action or economic coercion – could outweigh the perceived benefits of conducting cyber attribution against active cyber actors like China, Russia or North Korea. This presents a serious challenge to implementing a pan-ASEAN cybersecurity or cybercrime framework.

Existing 'minilateral' arrangements, such as the Indonesia-Malaysia-Philippines (INDOMALPHI) Trilateral Cooperative Arrangement that seeks to enhance maritime domain awareness in the Sulu Sea and Sulawesi Sea, could offer insights on improving cybercrime co-operation among interested parties in Southeast Asia, while circumventing the current political gridlock in ASEAN. Being the Lead Shepherd for cybercrime, Singapore could push the formation of a similar minilateral grouping on cybercrime, grounded on shared interests and principles of pragmatism. Underscoring the economic incentives of reduced costs and improved digital trade could persuade Indonesia, Malaysia, Thailand, the Philippines and Vietnam to explore the possible formation of a co-operative agreement on cybercrime, while ASEAN as a group still decides its position on how to proceed with a region-wide cybercrime framework. Such a minilateral grouping on cybercrime could pilot policy approaches on mutual legal assistance and law enforcement measures that address thorny issues such as extra-territoriality or sovereignty.

Second, institutionalising a cybercrime working group through track 1.5 dialogue – a working group composed of experts and practitioners from government, private sector, academia, and civil society – that promotes increased interaction between the public and private sector should be pursued. Interpol and UNODC's collaboration with the tech sector offer wide-ranging perspectives on incorporating private sector perspectives to manage cybercrime from the onset. Engaging the tech, financial and banking sectors within policy discussions could alleviate institutional frictions that often derail real-time legal assistance to retrieve electronic evidence or preserve data. Likewise, the private sector's technical expertise can help inform and educate government policymakers, regulators, and law enforcement officers to improve their capacity in fighting cybercrime. It is only by bringing all parties to the table – government, the private sector, academia, and civil society, all with distinct capabilities – that full-scale analysis of cybercrime as a phenomenon will take place. By obtaining an accurate picture of the cybercrime threat landscape, concerned government agencies can then prioritise and direct their resources to address cybercrime incidents based on urgency and severity.

External peer-to-peer learning with Commonwealth countries

The peer-to-peer learning model should also strengthen Southeast Asia's resolve to reinforce its connection among its counterparts in South Asia, Africa, Latin America and even the neighbouring Pacific islands. The proposed regular exchanges among these regions and countries should help preserve and cultivate an inclusive environment at the multilateral level, to reinforce trust and confidence away from the prevailing strategic manoeuvres of the big powers.

As demonstrated by the case of Singapore and Ghana, there is an opportunity for small and medium-sized countries to support each other's representation and participation in international governing bodies like the ITU. Beyond the binary narrative of the digital 'haves and have nots', small and medium-power countries should band together based on mutual and pragmatic interests to maintain the relevance and neutrality of diplomatic platforms to achieve concrete outcomes. Institutionalising track 1.5 or track 2 dialogues could be the next step to elevating the current momentum of co-operation between Southeast Asia and Commonwealth countries. Convening government policy-makers, industry practitioners, academic experts and representatives from civil society organisations could offer the opportunity for a cross-sectoral dialogue that emphasises local perspectives.

At the strategic level, Interpol and UNODC could act as brokers to lay the groundwork for greater co-operation between Commonwealth countries and Southeast Asia. With Interpol's presence in Africa and ASEAN, it can gather a consortium of Southeast Asia and Commonwealth countries to formulate confidence-building measures through information sharing through formal channels, such as the ASEAN Regional Forum. As an exploratory project, creating a Points of Contact Directory between ASEAN and Commonwealth countries may help translate this vision of peer-to-peer learning or collaboration. At the working level, organising strategic dialogues that embed tabletop exercises or 'wargames' could help test concepts and pinpoint synergies, both in heightened situations or crisis or by simulating joint law enforcement operations. In addition to promoting cyber norms and the application of international law, regular dialogues can help clarify practical considerations for small and medium-sized countries participating in peer-to-peer learning initiatives given their limited resources and capacity.

Conclusion

Southeast Asia's promise to become a digital economic powerhouse not only provides the means to fast-track its economic recovery post-COVID, but also offers the region several opportunities to shape cyber diplomacy engagements on cybercrime at the regional – and potentially at the international – levels. Through the concept of peer-to-peer learning, technologically capable states like Singapore, Malaysia, Indonesia, Thailand, the Philippines, and Vietnam could bolster co-operation on cybercrime amid the absence of a region-wide approach and ASEAN's declining political and institutional powers.

Drawing insights from existing minilateral arrangements like INDOMALPHI can help encourage ASEAN to formulate collaborative and practical pathways to move forward in combatting cybercrime. The formation of minilateral groupings can also circumvent political deadlock and facilitate regional co-ordination and consultation on cybercrime. Operationally, such groupings could test pilot approaches on mutual legal assistance, involving law-enforcement agencies, financial regulators and cybersecurity experts – both from the public and private sectors. This concept of peer-to-peer learning can go beyond Southeast Asia and offers the region the opportunity to explore collaboration among other like-minded countries that are part of the Commonwealth and who share mutual interests in tackling cybercrime.

As international co-operation on cybercrime remains difficult, the co-operative dynamics between Southeast Asia and Commonwealth countries located in South Asia, Africa, Latin America and the Pacific could offer new ideas on cross-border co-operation on cybercrime. To make this happen, a strong network of experts and practitioners from government, the private sector, academia, and civil society will play a crucial role in designing level-headed and comprehensive exercises and initiatives to consequently influence and shape the cyber agenda at the political and technical levels of national governments. By leveraging the distinct expertise of key stakeholders from the private and public sectors in various jurisdictions through regular exchanges, it becomes plausible to analyse the evolving scale of cybercrime threats and consequently manage their risks. This will then allow governments to prioritise and direct resources that enhance cross-regional cybercrime co-operation and will especially benefit developing economies, despite the current fragmentation of global internet governance.

ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

Cybercrime and the Adoption of Artificial Intelligence Systems for Judicial Decision-Making in Criminal Justice Systems

Dan Jerker B. Svantesson[1]

Abstract

We are now at a stage where cybercrime is more impactful than ever, given the extent to which society operates online. At the same time, there have been significant advances in Artificial Intelligence (AI). Consequently, the temptation to turn to AI to improve the rate of prosecution and adjudication of cybercrime is natural. Clearly, resource limitation is a significant restricting factor; improved efficiencies here may help combat cybercrime.

However, the criminal justice system is one of society's most sensitive functions. Thus, we need to proceed with extreme caution when seeking to rely on AI to improve how we address cybercrime.

Focusing on cybercrime, this article seeks to examine the practicalities of developing guidelines on the adoption of AI systems for judicial decision-making in criminal justice systems.

1. Introduction

Multiple studies have demonstrated that only a small percentage of cybercrime is prosecuted and adjudicated.[2] The reasons for this include resource limitations and cybercriminals' possession of a level of technical expertise comparable with that of those working in cybersecurity. Technologies such as Artificial Intelligence (AI) can help prevent cybercrime by identifying future risks through examining trends in data from earlier cyber-incidents, enabling appropriate authorities to focus on and predict future cyber-attacks.

[1] Faculty of Law, Bond University (Gold Coast, Australia). Email: dasvante@bond.edu.au

[2] See for example Kleijssen, J. and Perri, P. (2017) 'Cybercrime, Evidence and Territoriality: Issues and Options', in M. Kuijer and W. Werner (eds) *Netherlands Yearbook of International* Law 47: 147–173.

Given how common it is today to pursue efficiency via technology, it is only natural to examine the extent to which AI can increase efficiencies in the fight against cybercrime. In doing so, this article approaches AI broadly by examining the adoption of AI systems for judicial decision-making in criminal justice systems.

Importantly, the criminal justice system is a particularly sensitive aspect of society. Consequently, it is critical that any AI-driven efficiencies pursued to address cybercrime are compatible with fundamental values such as the rule of law traditionally emphasised within the Commonwealth.

At the meeting of Commonwealth Law Ministers and Senior Officials in November 2019, it was recognised that not all Commonwealth member countries have access to the same level of technology in their justice systems. The Commonwealth Law Ministers acknowledged the need to remain informed of technological advances and their potential impacts, and stressed the importance of collaborating to increase the scale of knowledge exchange across the Commonwealth in relation to technology.

Law Ministers highlighted the importance of considering the ethical framework surrounding the implementation of new technologies in justice delivery. They supported the development of Commonwealth guidelines to underpin the use of algorithmic decision-making in the legal sphere, based on good practice across the Commonwealth, as well as the formulation of guidance to detail when the public ought to be informed that automated data-driven systems are being used to make decisions of legal consequence. At that occasion, Law Ministers requested the Commonwealth Secretariat to examine the practicalities of developing guidelines on ethical issues linked with the use of technology and to report at the next Commonwealth Law Ministers Meeting (CLMM). As a result, a paper on the adoption of AI systems for judicial decision-making in criminal justice systems was presented at the November 2022 CLMM in Mauritius. At the 2022 CLMM, Law Ministers mandated the Secretariat to adopt a holistic approach to AI in the sector. In particular, the Secretariat should scope emerging practices on the use of AI across the Commonwealth and consider developing principles that align with Commonwealth values and principles.

Within the context of cybercrime, this article seeks to outline current uses of AI systems for judicial decision-making in criminal justice systems, the perceived benefits of such uses, and the risks and challenges involved.

2. Context

The current pandemic has brought about what may be termed a 'COVID-driven trend acceleration' – that is, already existing trends are significantly accelerated because of the COVID-19 pandemic and how society is adjusting to it. One aspect of this is society's increased reliance on the online environment. Put simply, information technology is playing an important role in society. With this come increased opportunities for cybercriminals. This situation also means that cybercrime has a larger societal impact. Thus, it may be argued that it has never been more important to effectively address cybercrime.

The COVID-driven trend acceleration can also be seen in developments in, and the adoption of, AI as a part of this broader and intensified technological uptake. However, AI already has quite a long history.

2.1 A background to AI

AI has been discussed with varying degrees of intensity since the early 1950s.[3] However, significant advances in computing power, data analysis techniques, natural language processing and the availability of large datasets have recently transformed the AI landscape and brought about rapid progress. Despite the attention directed at AI, there are no universally accepted definitions, and AI is not a homogeneous object. However, common themes in discussions of AI focus on the ability to 'mimic human thought'[4] and thereby the capacity to carry out tasks previously falling within the exclusive domain of human capability. The Council of Europe's Ad Hoc Committee on Artificial Intelligence, for example, has concluded that:

> *the term 'AI' is used as a 'blanket term' for various computer applications based on different techniques, which exhibit capabilities commonly and currently associated with human intelligence. These techniques can consist of formal models (or symbolic systems) as well as data-driven models (learning-based systems) typically relying on statistical approaches, including for instance supervised learning, unsupervised learning and reinforcement learning. AI systems act in the physical or digital dimension by recording their environment through data acquisition, analysing certain structured or unstructured data, reasoning on the knowledge or processing information derived from the data, and on that basis decide on the best course of action to reach a certain goal. They can be designed to adapt their behaviour over time based on new data and enhance their performance towards a certain goal.*[5]

[3] See in particular Turing, A. (1950) 'Computing Machinery and Intelligence', in R. Epstein, G. Roberts and G. Beber (eds) (2009) *Parsing the Turing Test*. Dordrecht: Springer; McCarthy, J., Minsky, M., Rochester, N. and Shannon, C. (1955) 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence'. Reprinted in AI Magazine 27(4) (2006).

[4] Simon McDougall, S. (2019) 'Developing the ICO AI Auditing Framework: An Update'. UK Information Commissioner's Office, 4 July. https://ico.org.uk/about-the-ico/news-and-events/ai-blog-developing-the-ico-ai-auditing-framework-an-update/

[5] Council of Europe Ad Hoc Committee on Artificial Intelligence (2020) 'Feasibility Study CAHAI(2020)23'. Strasbourg, 17 December. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

Change – in the form of AI adoption – is already ongoing and, as is often the case, we are in a situation where regulation is trying to 'catch up' with technological advances. However, especially in the context of criminal justice systems, doubt has been cast on how much in this evolution is driven by societal needs as opposed to by marketing and the industry.[6]

Furthermore, given the seemingly undisputed fact that AI will continue to evolve, the task before us is not merely to ensure that regulation catches up with AI technology. It also involves setting rules and standards now that can guide and regulate the adoption of AI systems for judicial decision-making in criminal justice systems on an ongoing basis. Put simply, this is not a task that can be addressed to completion at this stage; it will require an ongoing commitment, monitoring and review.

2.2 AI and the judicial system

The judicial system is a part of society and, as such, it should evolve with the rest of society, including when it comes to technological developments. However, technological development, such as the adoption of AI systems, is not in itself a goal for the criminal justice system. Rather, it is the potential that AI systems hold to facilitate recognised goals such as efficiency increases, cost minimisation and improved access to justice that makes it a topic worthy of consideration.

Any discussions of technological reform to judicial decision-making in criminal justice systems must start with the realisation that the justice system is a sensitive core function of society and thus it is something that requires particular care.[7] As a result, technological progress is clearly less important than is the integrity of the system, and progress being slower in relation to the adoption of AI in the judicial system, compared with for less sensitive societal functions, is both natural and desirable. This means that solutions that may be viewed as appropriate in less sensitive areas may not be suitable for how the criminal justice system addresses cybercrime or, indeed, for the criminal justice system as a whole.

[6] For example, the European Commission for the Efficiency of Justice prompts us to 'differentiate between this commercial discourse and the reality of the use and deployment of these technologies' (European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment, 31st Plenary Meeting, 3–4 December 2018. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c). The 'hype' around AI is well illustrated in the following statement made in 1960: 'Within the very near future – much less than twenty-five years – we shall have the technical capability of substituting machines for any and all human functions in organisations. ... Duplicating the problem-solving and information-handling capabilities of the brain is not far off; it would be surprising if it were not accomplished within the next decade" (see further the discussion of this 'over-enthusiasm' (Clarke, R., 2019, 'Guidelines for the Responsible Business Use of AI'. Foundational Working Paper Revised Version of 20 February 2019. Xamax Consulting Pty Ltd. www.rogerclarke.com/EC/GAIF.html).

[7] The need to impose strict requirements on judicial decision-making in criminal justice systems is widely accepted. See for example the emphasis on independence, impartiality, integrity, propriety, equality, competence and diligence in the United Nations Bangalore Principles of Judicial Conduct (see UNODC, 2007, *Commentary on the Bangalore Principles of Judicial Conduct*. Vienna: UNODC).

2.3 An enabling framework safeguarding key values

The main message of this article is that, to increase efficiencies in addressing cybercrime, there is a need for a clear framework – preferably at the Commonwealth level – that enables developments for the adoption of AI systems for judicial decision-making in criminal justice systems to take place in a safe, accountable and rights-respecting manner safeguarding the values of the Commonwealth, including the rule of law as an essential protection for the people of the Commonwealth and as an assurance of limited and accountable government. In particular, despite the importance of addressing cybercrime, AI systems should not be adopted in a manner that undermines an independent, impartial, honest and competent judiciary or the independent, effective and competent legal system as an integral component in upholding the rule of law, engendering public confidence and dispensing justice.

The design of such a framework is a task for all Commonwealth member countries equally, regardless of their current state of technological[8] and policy[9] development. Too often, a small number of the most technologically advanced countries set technological and regulatory developments for all countries.[10] By adopting the inclusive and multistakeholder approach to which the Commonwealth is already committed,[11] and by doing so at this early stage of the development of the adoption of AI systems for judicial decision-making in criminal justice systems, a more equitable and better-informed direction can be set.

2.4 Necessity and urgency

What is at stake in the context of the adoption of AI systems for judicial decision-making in criminal justice systems is nothing less than the following six matters of fundamental importance for all Commonwealth member countries:

[8] Unequal access to the Internet remains a major concern. For example, 'Only 40% of Africans have access to the Internet today, compared to 87% in Europe and 95% in North America' (Candelon, F., El Bedraoui, H. and Maher, H. (2021) 'Developing an Artificial Intelligence for Africa Strategy'. OECD Blog, 9 February. https://oecd-development-matters.org/2021/02/09/developing-an-artificial-intelligence-for-africa-strategy/). See more generally the AI Readiness Index 2020 of Oxford Insights and the International Research Development Centre (www.oxfordinsights.com/government-ai-readiness-index-2020).

[9] While some Commonwealth member countries (especially Canada and Singapore) have been world-leading adopters of AI strategies and policies, others are yet to develop such instruments. And, indeed, many still lack strategies and policies for the digital economy more broadly. For example, it has been noted that, 'While most Caribbean economies have developed broad ICT [information and communication technology] policies and strategies throughout the years, very few have developed targeted policies specifically addressing aspects of the digital economy' (Brathwaite, C., 2020. 'Artificial Intelligence & The Caribbean: A Discussion Paper on (Potential) Applications & Ethical Considerations', in C. Aguerre (ed.) *Inteligencia Artificial en América Latina y el Caribe. Ética, Gobernanza y Políticas*. Buenos Aires: CETyS Universidad de San Andrés).

[10] Svantesson, D. (2019) *Internet & Jurisdiction Global Status Report 2019*. Paris: Internet & Jurisdiction Policy Network.

[11] See for example the Commonwealth Cyber Declaration 2018 (https://thecommonwealth.org/commonwealth-cyber-declaration-2018).

1. justice in individual cases
2. the protection of fundamental human rights
3. upholding human dignity
4. adherence to the rule of law
5. what qualifies as a source of law and
6. trust in the legal system.

Given the fundamental significance of these matters, regulation by law is a necessity.[12] The types of ethics-focused guidelines and standards that have preceded discussions of regulation by law remain useful but are no substitutes for regulation by law for such sensitive matters. Thus, the legal regulation of AI systems for judicial decision-making in criminal justice systems is an issue on which Law Ministers may wish to start reflecting now, even where they are not currently in the process of actually adopting such systems in the pursuit of better addressing cybercrime.

3. Uses, including selected illustrative examples

When it comes to the uses to which AI may be put to address cybercrime, it must be understood that much of the discussion is focused on the adoption of AI systems for judicial decision-making in criminal justice systems in a technology-neutral manner as far as the types of crime are concerned. In other words, the efficiency impact of AI is generally pursued across all criminal activities, not specifically for cybercrime.

As this article addresses the adoption of AI systems for judicial decision-making in criminal justice systems, it is prudent to pay attention to the meaning of 'AI systems for judicial decision-making'. In this context, we may note the Australian Human Rights Commission's useful definition of 'AI-informed decision making' as a 'decision or decision-making process that is materially assisted by the use of an AI technology or technique and that has a legal, or similarly significant, effect for an individual'.[13]

As also noted by the Australian Human Rights Commission, 'In some cases, the use of AI will be central to the decision-making process, and the ultimate decision. For others, AI will have only a trivial impact on the decision-making process.'[14] This is an important observation that brings attention to the need for an appropriate analytical granularity and to the fact that each use must be evaluated individually.

[12] For an example of an attempt at comprehensively regulating AI, see Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final.

[13] Australian Human Rights Commission (2021) *Human Rights & Technology Final Report* (p. 38).

[14] Ibid. (p. 39).

The types of uses to which AI has been, and is anticipated to be, put into service within the context of judicial decision-making in criminal justice systems are diverse. In part, this is a consequence of AI not being a homogeneous object. However, it may also be explained by the fact that this is very much a developing field. Indeed, an examination of the extent to which Commonwealth member countries have already adopted AI systems for judicial decision-making in criminal justice systems provides few examples. This is also the case more broadly.[15] For example, the European Commission for the Efficiency of Justice (CEPEJ) notes that, 'For the time being judges in the Council of Europe member states do not seem to be making any practical and daily use of predictive software.'[16] In the literature, much of the discussions are focused on examples from the United States.

Nevertheless, it is possible to discern six different types of uses that warrant mentioning. These uses take place in different settings and at different points in time in the judicial process, but some may apply in parallel.

3.1 AI systems adopted to support the administration of the judicial process

AI systems can be adopted to support the administration of the judicial process. Such systems can, for example, make case management more efficient, and perform evaluations supporting budget and resource predictions. This may be particularly relevant in the context of cybercrime, given the very small percentage of cases prosecuted and adjudicated.

AI systems can also be adopted to support the administration of the judicial process in the form of tools for providing, and making more accessible, legal information, for example via 'chatbots' capable of providing tailored information. One provider describes the functionality of its Artificially Intelligent Legal Information Research Assistant in the following: 'You chat with her just as you a human lawyer. You can ask her questions, and she may ask you questions back to help guide you to helpful legal information. She can help you create documents, and if need be speak with a human lawyer to review those documents and information provided to you.'[17] As victims of cybercrime already are online, such resources may be particulary relevant for such victims.

[15] 'The number of cases in which AI programs have actually been used as a support tool for adjudication does not amount to more than can be counted on the fingers of one hand' (Caianiello, M., 2021, 'Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice'. *European Journal of Crime, Criminal Law and Criminal Justice* 29: 1-23, p. 3).

[16] CEPEJ (2018) 'European Ethical Charter' (p. 14).

[17] www.ailira.com/

Steps like these may strengthen access to justice and cut costs. Adopted in these roles, AI systems introduce limited risks, although, as discussed below (Section 5), risks still exist and must be managed. After all, decisions made about the judicial process, such as the case allocation to specific judges, for example, may be biased, discriminatory and violate fundamental rights relating to procedural fairness.

3.2 AI systems providing decision-making support

AI systems may provide decision-making support. This can take different forms, some of which we are already familiar with, such as information systems (e.g. advanced case law search engines).[18] Others, such as analytical functions and, for example, the use of AI systems to propose possible interpretations of ambiguous terms or statutory provisions, take us into a 'grey zone' between AI systems providing decision-making support and such systems becoming co-adjudication, as discussed directly below. The same is true in relation to AI systems used for 'judge profiling', for example in the form of offering judges detailed quantitative and qualitative assessment of their own activities to help them self-identify patterns indicative of biases. The European Commission for the Efficiency of Justice suggests that, used purely for the informative aim of assisting in decision-making and for the judges' own exclusive use, such profiling could be encouraged.[19]

3.3 AI systems utilised for co-adjudication

AI systems, adopted in the context of judicial decision-making in criminal justice systems, can be utilised for co-adjudication – that is, judicial decisions are made by a human judge together with the AI system. This usage can, for example, include the AI system drafting decisions that are approved and edited by a human judge, or the AI system proposing alternative options based on pre-set criteria and highlighting the most 'suitable' based on those criteria while also ranking the degree of criteria fulfilment of other outcomes.

3.4 AI systems as 'robot judges'

The most advanced form of AI system use in the context of judicial decision-making in criminal justice systems is the 'robot judge'. A robot judge would be an AI system that directly and autonomously adjudicates matters. This is not a current usage but it needs to be flagged here as such a development is part of the discussions of AI systems for judicial decision-making in criminal justice systems. Any application of robot judges in the context of cybercrime must be guided by the sensitivity of the criminal justice system.

[18] CEPEJ (2018) notes, 'The use of machine learning to constitute search engines for case-law enhancement is an opportunity to be taken up for all legal professionals' ('European Ethical Charter', p. 63).

[19] CEPEJ (2018) 'European Ethical Charter' (p. 66).

3.5 AI systems in alternative dispute resolution structures

While more prominent outside the criminal justice system, some forms of alternative dispute resolution (ADR) – like restorative justice – may be used in the context of decision-making in criminal justice systems, potentially also in relation to cybercrime. As AI systems may play a direct or supporting role in various ADR structures, this usage must be noted.

3.6 AI systems facilitating predictive policing, preventative justice and pre-trial risk assessment

The use of AI systems to facilitate so-called 'predictive policing', 'preventative justice'[20] and 'pre-trial risk assessment' may play a role in more than one of the five categories outlined above, and has attracted much attention in the literature.[21] This is only natural given that this is a setting in which there are examples of both adopted systems and systems being tested. At the same time, it may be noted that predictive policing does not need to depend on AI systems, but rather can be carried out entirely by human intelligence. At any rate, the Australian Human Rights Commission notes:

> *Data-driven risk assessment tools are used increasingly to predict the likelihood of future criminal behaviour. These tools are starting to be rolled out in a number of countries to assist decision making in the criminal justice system, including decisions regarding sentencing, bail and post-sentence restrictions on people assessed as being likely to commit further crime.*[22]

The best-known instances of predictive policing relate to physical crime rather than cybercrime. Perhaps the most familiar of these data-driven risk assessment tools, outside the United States, is the Harm Assessment Risk Tool (HART) developed by the

[20] The term 'predictive justice' has been criticised as being 'dangerously misleading' since 'such systems make predictions, but not judicial decisions. Judicial decisions require, as a minimum standard, justifications based on an assessment of the relevant facts and applicable regulations. AI systems make statistical correlations and their forecasts are just the result of those correlations. Hence, it would only be proper to speak of actual predictive justice if the systems were to provide justifications in terms of facts and laws' (Contini, F., nd, 'Artificial Intelligence: A New Trojan Horse for Undue Influence on Judiciaries?' https://www.unodc.org/dohadeclaration/en/news/2019/06/artificial-intelligence_-a-new-trojan-horse-for-undue-influence-on-judiciaries.html).

[21] See for example Ashworth, A. and Zender, L. (2014) *Preventive Justice*. Oxford: Oxford University Press; Lynskey, O. (2019) 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing'. *International Journal of Law in Context* 15(2): 162–176. Most pretrial risk assessment tools try to estimate 'recidivism risk' (i.e., how likely a person is to commit a crime or be arrested) and 'flight risk' (i.e., how likely a person is to not show up at trial) (EPIC, 2020, *Liberty at Risk: Pre-trial Risk Assessment Tools in the U.S.* Washington, DC: EPIC).

[22] Australian Human Rights Commission (2021) *Human Rights & Technology Final Report* (p. 43).

University of Cambridge in collaboration with Durham Constabulary.[23] HART is based on a machine-learning algorithm to aid decision-making by custody officers when assessing the risk of future offending.[24] In more detail:

> *the AI-based technology uses 104,000 histories of people previously arrested and processed in Durham custody suites over the course of five years, with a two-year follow-up for each custody decision. Using a method called 'random forests', the model looks at vast numbers of combinations of 'predictor values', the majority of which focus on the suspect's offending history, as well as age, gender and geographical area. …*
>
> *The aim of HART is to categorise whether in the next two years an offender is high risk (highly likely to commit a new serious offence such as murder, aggravated violence, sexual crimes or robbery); moderate risk (likely to commit a non-serious offence); or low risk (unlikely to commit any offence).*[25]

Other noteworthy data-driven risk assessment tools include Connect, widely used by UK police[26] and recently commissioned for the Jamaican police force,[27] the New South Wales Police Force's Suspect Targeting Management Plan (STMP)[28] and Interpol's International Child Sexual Exploitation Database.[29] The latter is an intelligence and investigative tool with an image and video database that allows specialised investigators to share data on cases of child sexual abuse:

> *Using image and video comparison software, investigators are instantly able to make connections between victims, abusers and places. The database avoids duplication of effort and saves precious time by letting investigators know whether a series of images has already been discovered or identified in another country, or whether it has similar features to other images.*

It also allows specialized investigators from more than 64 countries to exchange information and share data with their colleagues across the world.

[23] University of Cambridge (2018) 'Helping Police Make Custody Decisions Using Artificial Intelligence'. 26 February. www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence

[24] Oswald, M., Grace, J., Urwin, S. and Barnes, G. (2018) 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality'. *Information & Communications Technology Law* 27(2): 223–250 .

[25] University of Cambridge (2018) 'Helping Police Make Custody Decisions'.

[26] For further details, see the provider's website: www.necsws.com/solutions/police-software/police-record-management-system/

[27] Booth, F. (2021) 'Jamaican Police Force Adopts Technology Platform in Drive to Combat Crime'. NEC Insights, 6 July. www.necsws.com/news/jamaican-police-adopts-technology-platform/

[28] See further Yeong, S. (2020) 'An Evaluation of the Suspect Target Management Plan'. Crime and Justice Bulletin No. 233 Revised. Sydney: NSW Bureau of Crime Statistics and Research; Sentas, V. and Pandolfini, C. (2017) 'Policing Young People in NSW: A Study of the Suspect Targeting Management Plan'. Report of the Youth Justice Coalition NSW. Sydney: Youth Justice Coalition NSW.

[29] See further www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database and the discussion in Završnik, A. (2020) 'Criminal Justice, Artificial Intelligence Systems, and Human Rights'. *ERA Forum* 20: 567–583 https://doi.org/10.1007/s12027-020-00602-0

> *By analysing the digital, visual and audio content of photographs and videos, victim identification experts can retrieve clues, identify any overlap in cases and combine their efforts to locate victims of child sexual abuse.*[30]

Importantly, predictive policing may have particular future application in relation to cybercrime, for example based on spatial studies of cybercrime perpetrators and cybercrime victims. This is certainly a topic that requires further academic attention.

4. Perceived benefits

An examination of policy documents and academic literature shows considerable consistency in the perceived benefits associated with the adoption of AI systems for judicial decision-making in criminal justice systems. Some such benefits are clearly related, and partly overlapping. For example, increased efficiency may lead to cost reductions and may, at the same time, facilitate greater access to justice that caters for greater equality. However, whether talking of increased efficiency or related cost reduction, it may be said that the common denominator is the potential to enhance access to justice, clearly a key issue in the context of cybercrime.

4.1 Three forms of enhanced access to justice

With its strong and clearly articulated commitment to, and focus on, facilitating access to justice,[31] it is important that the Commonwealth explore options for the adoption of AI systems for judicial decision-making in criminal justice systems. Considering the uses described in Section 3, AI systems have the potential to enhance access to justice in at least three different ways: (i) improved access, and improved quality of that access, to legal information; (ii) greater procedural efficiency leading to, for example, shorter waiting times; and (iii) increased quality of judicial decision-making. These forms of enhanced access to justice are as relevant for cybercrime as they are for offline crimes.

The first two of these ways in which AI systems may enhance access to justice are rather self-explanatory. However, a few observations must be made about the third. One aspect of the potential for increased quality of judicial decision-making is found in that AI systems may be used to identify, minimise and even eliminate human biases.

[30] www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

[31] See for example Latu-Sanft, J. (2019) 'Commonwealth Law Ministers Resolve to Take Action on Access to Justice'. News, 7 November. https://thecommonwealth.org/media/news/commonwealth-law-ministers-resolve-take-action-access-justice.

4.2 Identifying, minimising and eliminating human biases

Decisions made by humans may be made based on conscious or subconscious biases, and those mental shortcuts that form a natural part of human reasoning.[32] AI systems may be used to address such issues in at least two different ways. First, where AI makes the decisions, such direct human biases are eliminated (although, as discussed below, AI systems may also introduce, or re-introduce, biases).

Second, AI systems may be used to analyse human decisions with the aim of identifying biases. This may be done at the time of the decision-making process, thereby giving the decision-making person the opportunity to become aware of biases and alter the decision before it is finalised. However, AI-based identification of human biases may also be utilised after decisions have been made in a monitoring/review context.

4.3 Other potential benefits

Other potential benefits that the adoption of AI systems for judicial decision-making in criminal justice systems may provide include certainty, equality, consistency, predictability and transparency, resulting in higher quality in judicial decision-making.[33] For example, AI systems may help eliminate excessive variability in court decisions,[34] thus supporting the principle of equality before the law.

5. Identified risks and challenges

As with the perceived benefits discussed above, an examination of policy documents and academic literature shows considerable consistency in the identified risks and challenges associated with the adoption of AI systems for judicial decision-making in criminal justice systems.

5.1 AI systems and legal authority

A fundamental consideration for any adoption of AI systems for judicial decision-making in criminal justice systems stems from the limits on legal authority – that is, can AI systems have legal authority in the judicial decision-making in criminal justice systems?[35] Without such legal authority, their use must always be limited to a support function. The way in which this restriction has been managed is through 'delegated authority',[36] but

[32] Završnik (2020) 'Criminal Justice'.

[33] See for example Caianiello (2021) 'Dangerous Liaisons'.

[34] Re, R. and Solow-Niederman, A. (2019) 'Developing Artificially Intelligent Justice'. *Stanford Technology Law Review* 242–289.

[35] Sourdin, T. (2018) 'Judge v Robot? Artificial Intelligence and Judicial Decision-Making'. *UNSW Law Journal Volume* 41(4): 1114–1133.

[36] For a possible example of this, see Australia's Therapeutic Goods Act 1989 (Cth) s 7C(2) discussed in Sourdin (2018) 'Judge v Robot?'.

different legal systems may impose different limitations on the delegation of decision-making power to machines. Ensuring authority may be particularly complicated in the context of cross-border crime, as often is the case in cybercrime.

5.2 Distinction between outcome and process – human dignity and the risk of alienation

Another issue of overriding importance is the distinction between outcome and process. Even where AI systems are capable of producing results akin to those of a human judge, those systems make no attempt to formalise legal reasoning. Rather, the developers create models aimed at anticipating the likely decisions of a judge in similar situations.[37] Given the important role played by the process itself in judicial decision-making in criminal justice systems – including for cybercrime – it may be argued that AI systems are incapable of meeting certain fundamental rights standards, such as those relating to procedural fairness, and that being judged by a machine undermines human dignity. This points to a need for a deeper discussion of a potential right to be judged by a human. Relatedly, commentators have pointed to the risk of AI systems causing a sense of alienation in relation to the legal system.[38]

5.3 AI systems creating a new, unintentional, source of law?

Another challenge that calls for deeper discussions is the potential for AI systems to, in a sense, create a new source of law. Some commentators have pointed to the risk of 'datafication' – that is, 'by focusing attention on seemingly objective data and adapting legal systems to incorporate this information, "datafication," or emphasis on available data and its uses, might undesirably influence the legal system's operation'.[39] Similarly, as noted by CEPEJ, 'Thought should be given to the transformation of the very logic of the production of case-law. What is the value of the "standard" resulting from the number of decisions given on a specific matter? Does this "standard" add to the law? If so, is this a new source of law?'[40] Put differently, will AI systems turn quantitative caselaw statistics into a source of law? And, if so, how will that source relate to the more qualitative case law usage typical of human judges? Further, the AI systems' quantitative treatment of case law may impact court hierarchy and the court system, as such:

> *would it not be the case that if norms were established according to the majority trend, judicial decisions would be rendered uniform, and no longer be ordered according to the hierarchy of the courts from which they emanate, disregarding the significance of the decisions of supreme courts, which are the guarantors of the uniform interpretation of law in many … States?*[41]

[37] CEPEJ (2018) 'European Ethical Charter'.

[38] Re and Solow-Niederman (2019) 'Developing Artificially Intelligent Justice'.

[39] Ibid. (p. 267).

[40] CEPEJ (2018) 'European Ethical Charter' (p. 23).

[41] Ibid. (p. 24).

Perhaps there is such a thing as 'excessive standardisation of judicial decisions'[42] and perhaps such excessive standardisation is more likely to cause inequality than it is to cater for equality. All this is particulary sensitive in the context of the criminal justice system, including in its application to cybercrime.

5.4 AI systems and the need for discretion

Some commentators[43] have pointed to the prevalence of discretion in adjudication stemming from, for example, the 'under-determinate' nature of law. They highlight the important role of discretion and question whether AI systems can fulfil the aspects of adjudication that involve discretion.[44] In addition, we may question whether AI systems *should* handle the aspects of adjudication that involve discretion or whether such discretion must always be exercised by a human. This is a most significant question. If the answer is that such discretion must always be exercised by a human, the result seems to be that, for most purposes falling within the context of judicial decision-making in criminal justice systems, AI systems may not be used as an autonomous 'robot judge' but may be used only for, for example, co-adjudication and decision-making support.

5.5 The risk of disillusionment

It has also been observed that the adoption of AI systems for judicial decision-making may cause disillusionment in relation to human judges and the legal system more broadly – that is, where an AI system highlights flaws and biases in the decisions of human judges, a resulting 'disillusionment would erode confidence in the legal system's legitimacy. Insofar as increasing use of AI adjudication prompts people to look more skeptically [sic] at human judging, the legitimacy of existing legal activities could be cast into doubt.'[45]

5.6 A lack of transparency

One of the most frequently noted risks with AI systems for judicial decision-making, including in the context of criminal justice systems applied in the cybercrime context, is that stemming from AI creating a lack of transparency. This is not a setting in which a 'black box' effect[46] – put simply, opacity in the step between input and output in a decision-making process – can be accepted. Decisions made in the criminal justice context must be explainable to those directly affected. This is essential, for example

[42] Ibid.

[43] See for example Završnik (2020) 'Criminal Justice' (pp. 580–581).

[44] 'Removing human discretion thus is a double-edged sword: it can reduce human bias, but it can also exacerbate past injustices or produce new ones' (Završnik, 2020, 'Criminal Justice', p. 581).

[45] Richard M. Re & and Alicia Solow-Niederman (2019,) 'Developing Artificially Intelligent Justice', 22 STAN. TECH. L. REV. 242 (2019), at (p. 273).

[46] See for example NITI Aayog (2018) 'National Strategy for Artificial Intelligence'. Discussion Paper. https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf; Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

to ensure that informed decisions can be made about whether a person accused of committing cybercrime should appeal the decision, and if so on what grounds, but also more generally for the dignity of the affected party. Such decision must also be explainable to society at large so that the overall fairness and equality of the system may be monitored.

5.7 AI systems and biases

Another frequently highlighted concern with AI systems for judicial decision-making, not least in criminal justice systems, relates to biases. As noted in Section 4, AI systems may be used to identify and even eliminate human biases. But AI systems may also introduce biases in at least three forms. First, any human biases of the creators of the AI system may be transmitted into the AI system as such ('creator biases').[47] Second, the selected training data for an AI system may significantly affect the system's operation, and any intentional or unintentional biases in the data may contaminate how the system operates ('data-driven biases'). In this context, specific mention must be made of the risk that biases that society has moved past are reintroduced where old data (i.e., data that predate the change away from that bias) are used. Third, systems that evolve, such as forms of machine learning, may develop biases over time ('systems-driven biases').

The obvious concern about these types of biases is that they may result in discrimination between individuals and groups of individuals. This is a key concern in the context of the adoption of AI systems for judicial decision-making in criminal justice systems, including in the context of cybercrime. However, such biases are not the only way in which discrimination may arise. As the Australian Human Rights Commission notes, 'Poor technology design can exclude people with disability from work, services and the economy.'[48] In other words, in order to avoid discrimination, technology must be made accessible to all regardless of factors such as level of education, gender, economic position, demographics and disabilities.

5.8 Technology dependence and the 'digital divide'

Increases in technology dependence – including the adoption of AI systems for judicial decision-making in criminal justice systems – may augment the so-called 'digital divide' – that is, the gap between those with reliable access and those who lack reliable access to the technology. The digital divide may stem from a range of sources, such as gender, location, level of education and differences in the available Internet architecture, and may exists on several levels, including between individuals, groups and countries.[49]

[47] 'The neutrality of algorithms is a myth, as their creators consciously or unintentionally transfer their own value system into them' (CEPEJ, 2018, 'European Ethical Charter', p. 57).

[48] Australian Human Rights Commission (2021) *Human Rights & Technology Final Report* (p. 7).

[49] See for example Sibal, P. and Neupane, B. (2021) *Artificial Intelligence Needs Assessment Survey in Africa*. Paris: UNESCO.

5.9 Function creep' and AI systems as an unintended de facto judge

A further concern that has been expressed in relation to the adoption of AI systems for judicial decision-making in criminal justice systems is the risk of so-called 'function creep'.[50] Put simply, function creep occurs where the use or application of a system or technology expands beyond its original purposes.[51] This is a commonly articulated concern in the intersection between law and technology. In the context of judicial decision-making in criminal justice systems, function creep may occur on several levels. For example, systems implemented for decision-making support may end up being used as co-adjudicators, and systems implemented for co-adjudication may end up being used as the main adjudicator.

A partially overlapping risk is that of overreliance making AI systems the *de facto* judge even where the AI system is only meant to be a co-adjudicator or to provide decision-making support. This risk stems from the fact that human judges may experience fear of departing from AI-guided draft decisions or recommendations.[52] Put simply, where a human judge follows a draft decision or recommendation made by an AI system, errors in that decision may be 'blamed' on the AI system. In contrast, where a human judge departs from a draft, proposal or recommendation made by an AI system, errors in the judge's decision may be 'blamed' on the judge in question, and the sense of blame may be intensified by the very fact that the judge did not follow the proposal made by the AI system.

5.10 AI systems as 'self-fulfilling prophecies'

Fears have been expressed about the potential for AI systems to become what may be labelled 'self-fulfilling prophecies'. This may be the case where an error, or misjudgement, made somewhere in the process, becomes incorporated in a decision that then forms the basis for future decision-making. In this context, the difficulty of identifying and eliminating false correlations is noteworthy. For example, a system that identifies a pattern of cyber-fraud conducted by persons with a name starting with a particular letter may assume a correlation between the first letter of names and the propensity to commit cyber-fraud. Put in the context of predictive policing, this may raise issues of confirmation bias. To continue the example above, the AI system's false correlations between the first letter of names and the propensity to commit cyber-fraud may cause investigative resources to be directed towards individuals whose name starts with the relevant letter. Such increased scrutiny is likely to result in a greater number of cyber-fraudsters being found among the group subjected to the increased scrutiny and the AI system is then proven 'right' even though the same result may have been reached regardless of which letter was in focus.

[50] Završnik (2020) 'Criminal Justice'.

[51] Koops, B.J. (2021) 'The Concept of Function Creep'. *Law, Innovation and Technology* 13(1): 29–56.

[52] See further CEPEJ (2018) 'European Ethical Charter'.

5.11 AI systems and the many roles of the judge

Commentators have also pointed to the multiple roles fulfilled by human judges.[53] For example, the role of a judge goes beyond dispute resolution to include activities such as education activities and social commentary. It seems clear that AI systems are not positioned to replace the human judge for such activities.[54] However, this may be a relatively minor issue since human judges can carry on with those activities even if complemented by AI systems. More importantly, concerns may be expressed about AI systems' argued inability to assess the social impact of their decisions and inability to ensure protection of societal values.

5.12 AI systems and the many roles of the law

It must be noted that the law fulfils multiple roles, and AI systems' ability to provide outputs that go beyond the case at hand has been called into question. Without going to deep into the quagmire of legal philosophy, it may be suggested that the law fulfils three different roles: it is a tool to (i) decide legal disputes, (ii) provide a framework to control, guide and plan life out of court and (ii) express and communicate the values of those who created the law.[55] For the second and third of these functions, the process and reasoning that led to the outcome (including what a judge states in *obiter*) are almost as important as the outcome itself. Doubt exists as to how capable AI systems are to fulfil these functions of the law.

5.13 A negative impact on fundamental rights and fundamental values

Much of the discussion of risks and challenges above one way or another relates back to concerns about the adoption of AI systems for judicial decision-making in criminal justice systems having a negative impact on fundamental rights, and fundamental values such as the rule of law. As already alluded to, several such rights are of relevance in the context of judicial decision-making in criminal justice systems – including in relation to cybercrime – and may be at risk as a result of the adoption of AI systems. Most obviously, principles of equality before the law, of the presumption of innocence, of the right to a fair and public hearing by a competent, independent and impartial tribunal established by law and of the right to be tried without undue delay are at stake. Article 14 of the International Covenant on Civil and Political Rights (ICCPR) is illustrative. It includes rights such as:

- All persons shall be equal before the courts and tribunals (14(1)).

[53] Sourdin (2018) 'Judge v Robot?'.

[54] Ibid.

[55] The first two of these roles may be derived from Hart, H., Raz, J. and Bulloch, P. (2012) *The Concept of Law*. 3rd ed. Oxford: Oxford University Press: 'The principal functions of the law as a means of social control are not to be seen in private litigation or prosecutions, which represent vital but still ancillary provisions for the failures of the system. It is to be seen in the diverse ways in which the law is used to control, to guide, and to plan life out of court' The third role is articulated in Svantesson, D. (2015) 'A Jurisprudential Justification for Extraterritoriality in (Private) International Law'. *Santa Clara Journal of International Law* 13(2): 517–552.

- Everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law (14(1)).
- Any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children (14(1)).
- There exists the right to be presumed innocent until proved guilty according to law (14(2)).
- There exists the minimum guarantee to be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him (14(3)(a)).
- There exists the minimum guarantee to have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing (14(3)(b)).
- There exists the minimum guarantee to be tried without undue delay (14(3)(c)).
- There exists the minimum guarantee to examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him (14(3)(e)).
- In the case of juvenile persons, the procedure shall be such as will take account of their age and the desirability of promoting their rehabilitation (14(4)).
- There exists the right to his conviction and sentence being reviewed by a higher tribunal according to law (14(5)).

There can be little doubt that the adoption of AI systems for judicial decision-making in criminal justice systems may be in conflict with obligations such as those noted above. Consequently, it is necessary to appreciate that these requirements are not obstacles for AI adoption; rather, their fulfilment is a necessary component of AI adoption in the pursuit of better addressing cybercrime.

In the context of the risk that AI systems may pose to fundamental rights, specific attention should also be given to the concerns that have been raised about how AI may affect data privacy. The data-intensive nature of AI is a direct threat to data privacy any time the data include 'personal data'.[56] Furthermore, as noted by the Council of Europe Ad Hoc Committee on Artificial Intelligence, 'A right to privacy implies a right to a private space free from AI-enabled surveillance as necessary for personal development and

[56] For a useful illustration of the relationship between data privacy law and AI, see Sartor, G. and Lagioia, F. (2020) 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence'. European Parliamentary Research Service, June. See also Gonzalez Fuster, G. (2020) 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights'. Study for the European Parliament (pp. 38–40).

democracy.'[57] There are, of course, many forms of 'AI-enabled surveillance', both for the online cybercrime environment and for the 'real' offline world. However, limiting the focus to the criminal justice systems context, some forms of predictive policing may fall within the category of AI-enabled surveillance.

5.14 Practical concerns

The above discussion of risks and challenges has focused mainly on risks posed by the adoption of AI systems for judicial decision-making in criminal justice systems, with an emphasis on the cybercrime context. Turning to challenges of a more practical nature, it may be noted that a study published in July 2021 points to data quantity, quality or availability as the main challenge in developing or deploying AI.[58] Other challenges noted in the same study include 'lack of available talent in the workforce', 'bias' and 'understanding appropriate governance and control'.[59]

Further, concerns have been expressed about intellectual property issues and security risks. The former relates to the impact that intellectual property and trade secret protection may have in preventing transparency. As to the latter, commentators have pointed both to risks of manipulation and to risks of disruption (e.g., via ransomware attacks).

6. Conclusion

Section 4, describing perceived benefits, demonstrates that there is a value in pursuing the adoption of AI systems for judicial decision-making in criminal justice systems as a tool to improve how we handle cybercrime. At the same time, given the sensitive nature of the AI uses discussed (Section 3) and taking account of the many well-founded risks and challenges outlined (Section 5), Law Ministers may wish to proceed with caution. Establishing a framework that enables developments to take place in a safe, accountable and rights-respecting manner may be regarded as an essential first step.

In the end, all the above may arguably be distilled into one thesis – that is, when adopting AI systems for judicial decision-making in criminal justice systems in the pursuit of important goals such as access to justice, it is necessary to ensure that the quality of the justice system is not compromised in the process. Thus, requirements imposed on AI systems, and their use, for judicial decision-making in criminal justice systems should not be viewed as obstacles to progress. Rather, such requirements – including those recommended in the section below – are necessary building blocks for the long-term

[57] Council of Europe Ad Hoc Committee on Artificial Intelligence (2020) 'Feasibility Study'.

[58] AI Asia Pacific Institute (2021) 'Trustworthy Artificial Intelligence in the Asia-Pacific Region'. July. https://aiasiapacific.org/wp-content/uploads/2021/07/2021-Trustworthy-Artificial-Intelligence-in-the-Asia-Pacific-Region.pdf (p. 20). As for access to data, it has been noted that, via the recourse to remote online legal proceedings, a wealth of new data is being generated that may serve to inform and train AI systems (Caianiello, 2021, 'Dangerous Liaisons', p.7).

[59] AI Asia Pacific Institute (2021) 'Trustworthy Artificial Intelligence' (p. 20).

success of AI systems for judicial decision-making in criminal justice systems in the fight against cybercrime. Against this background, it is now appropriate to present some recommendations on how we ought to proceed in this area.

7. Recommendations

A study of relevant policy documents, academic literature, ethical frameworks and proposed legal instruments shows a considerable degree of consistency in what is held to be required in the adoption of AI systems for judicial decision-making in criminal justice systems. Drawing upon such works, as well as the discussion above, several recommendations can be made for consideration by the Commonwealth member countries, and beyond. These recommendations are specifically discussed in the context of the adoption of AI systems for judicial decision-making in criminal justice systems in the fight against cybercrime. However, they ought to have equal applicability in any discussions of the adoption of AI systems for judicial decision-making in criminal justice systems. Indeed, the principles canvassed here should serve as a useful guide for any adoption of AI systems for judicial decision-making whether in the civil or the criminal justice systems.

As already alluded to, this article strongly advocates the creation of a clear framework that enables developments for the adoption of AI systems for judicial decision-making in criminal justice systems to take place in a safe, accountable and rights-respecting manner safeguarding the values of the Commonwealth,[60] including the rule of law as an essential protection for the people of the Commonwealth and as an assurance of limited and accountable government. AI systems aimed at combatting cybercrime should not be adopted in a manner that undermines an independent, impartial, honest and competent judiciary or the independent, effective and competent legal system as an integral component to upholding the rule of law, engendering public confidence and dispensing justice.

The Commonwealth Secretariat is well placed to play a crucially important role by facilitating the development of such a framework, whether it is ultimately articulated as a coherent Model Law at the Commonwealth level[61] or merely as model provisions recommended for consideration at a domestic level.

7.1 The fundamental rights principle

A framework for the safe, accountable and rights-respecting adoption of AI systems for judicial decision-making in criminal justice systems must be anchored in, and take care to integrate, international and domestic human rights law, and all other fundamental rights

[60] See for example the Commonwealth Cyber Declaration 2018, emphasising the 'Commonwealth values of human rights, tolerance, respect and understanding, freedom of expression, rule of law, good governance, sustainable development and gender equality'.

[61] See the Commonwealth Cyber Declaration 2018.

and values of free and democratic societies (the 'fundamental rights principle'). Several such rights are of relevance in the fight against cybercrime, including principles of equality before the law, of the presumption of innocence, of the right to a fair and public hearing by a competent, independent and impartial tribunal established by law and of the right to be tried without undue delay.

7.2 The rule of law principle

In addition, such a framework must be supportive of the multifaceted concept of the rule of law – both in the sense of directly supporting the rule of law and in the sense of working to enhance trust in the rule of law (the 'rule of law principle'). In fact, a rule of law focus may usefully be applied as a filter in the sense that any adoption of AI systems for judicial decision-making in criminal justice systems that supports the rule of law ought to be explored, and any adoption of AI systems in this setting that undermines the rule of law must be rejected even where they may otherwise prove effective tools against cybercrime – the cure should not be worse than the issue it seeks to address.

7.3 The lifecycle principle

Steps to guarantee adherence to, and support for, fundamental rights and the rule of law must be taken throughout the AI systems' entire 'lifecycle' (the 'lifecycle principle'), and that lifecycle may be split into a number of stages.[62] Thus, the regulation of AI in general, and the adoption of AI systems for judicial decision-making in criminal justice systems in particular, must be subject to ongoing monitoring, review and evaluation. This ongoing work should involve both public and private actors, and benefit from extensive consultation, audits, democratic scrutiny[63] and multistakeholder input. This is especially important in the context of cybercrime, where private actors play a significant role in how we respond.

7.4 The justification principle and the precautionary principle

Various tools may be pursued during the different stages of the AI lifecycle. For example, an important aspect in the 'design stage' is to promote responsible innovation through tools such as 'human rights by design', 'privacy by design' and 'ethical by design'. In addition, in relation to the 'deployment stage', Law Ministers may wish to consider and

[62] For example, a document published by The Alan Turing Institute speaks of the 'design stage', the 'development stage' and the 'deployment stage' (Leslie, D., Burr, C., Aitken, M. et al. (2021) 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law: A Primer'. The Council of Europe, pp. 10-12). Similarly, the Organisation for Economic Co-operation and Development speaks of four different phases: 'AI system lifecycle phases involve: *i)* "design, data and models"; which is a context-dependent sequence encompassing planning and design, data collection and processing, as well as model building; *ii)* "verification and validation"; *iii)* "deployment"; and *iv)* "operation and monitoring"' (OECD, 2019, 'Recommendation of the Council on Artificial Intelligence'. OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449).

[63] See for example the Montreal Declaration for a Responsible Development of Artificial Intelligence (www.montrealdeclaration-responsibleai.com/the-declaration), Principle 5.

adopt the 'justification principle' and the 'precautionary principle'. The justification principle means that, for any proposed adoption of AI systems for judicial decision-making in criminal justice systems, that proposal must be justified by reference to specific benefits and the achievability of the postulated benefits must be demonstrated. The justification principle will encourage a purposeful, rather than hype-driven, adoption of AI in this sensitive context. The precautionary principle signifies that, in any situation where it may reasonably be suspected that an AI system may cause harm, those proposing the adoption of the AI systems for judicial decision-making in criminal justice systems bear the burden to show that the system may be safely adopted. As one commentator notes, 'Ill-advised uses of AI need to be identified in advance and nipped in the bud, to avoid harm to important values.'[64]

In addition to these overriding considerations, a framework for the safe, accountable and rights-respecting adoption of AI systems for judicial decision-making in criminal justice systems may usefully incorporate several more specific key principles, many of which are recurring in the literature about the regulation of AI.

7.5 The appealability principle

Law Ministers may wish to consider and adopt the 'appealability principle' – that is, for any decision made by AI for the purpose of judicial decision-making in criminal justice systems, it must always be possible to appeal the decision to a human. In fact, Law Ministers may wish to consider embracing a ban on AI as final arbiter in the context of judicial decision-making in criminal justice systems in the context of both cybercrime and offline crime.

7.6 The explainability principle

Law Ministers may wish to consider and adopt the 'explainability principle' essential for the above-mentioned appealability principle, for upholding justice and dignity for those affected by a decision, and for facilitating society's monitoring of justice and equality in judicial decision-making. Under this principle, any decision made, or supported, by an AI system must be explainable to be valid. The principle covers both 'ex ante explainability' (i.e., the decision-making process being explainable prior to its use) and 'ex post explainability' (i.e., the decision-making process being explainable after its use).[65] This is particularly significant in the context of the adoption of AI systems for judicial

[64] Clarke (2019) 'Guidelines for the Responsible Business Use of AI'.

[65] 'Only some algorithmic methods lend themselves to ex ante transparency, notably those relying on decision trees. ... in the case of other algorithmic technologies, such as neural networks, the machine is learning as it processes the data and it is not possible to set out the reasoning in advance' (Black, J. and Murray, A., 2019, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda'. *European Journal of Law and Technology* 10(3)).

decision-making in criminal justice systems. Indeed, it may be said to flow from relevant fundamental rights. Adherence to the explainability principle may usefully incentivise further work on what has been termed 'explainable AI'.[66]

7.7 The transparency principle

Law Ministers may wish to consider and adopt the 'transparency principle'. This principle is related to, and partly overlaps with, the explainability principle. However, it does not only relate to the need for transparency in the sense of explainability. It also calls for transparency in the sense of persons being made aware of the fact that AI has played a role in a decision made about them, what methods were used and, at least, what parameters the AI system considered. Further, the transparency principle emphasises the need for law to clearly identify what decisions may be made by, or partially made by, AI systems. The transparency principle may be in tension with intellectual property and trade secret protections afforded to the developers of AI systems. In such situations, the rule of law demands that only systems that fulfil the transparency principle are adopted. This may be considered in the rules governing the procurement process of AI systems for judicial decision-making in criminal justice systems and may even point to a need to explore governments playing a role in the design and creation of AI systems for judicial decision-making in criminal justice systems.

7.8 The non-discrimination principle

Given the prominence of the risk of AI systems introducing, augmenting or re-introducing discrimination between individuals or groups of individuals, Law Ministers may wish to specifically consider and adopt the 'non-discrimination principle', requiring an ongoing commitment to eliminate discrimination, and risks of discrimination, in the adoption of AI systems for judicial decision-making in criminal justice systems. There are two dimensions to this principle. It aims to utilise AI systems to eliminate existing discrimination and it aims to prevent AI systems, one way or another, introducing discrimination. On a practical level, this may take several forms. For example, attention can be directed at what variables AI systems use as the basis for their decisions. Where the variables include examples of sensitive data, such as on gender, political opinions or ethnicity, that may be used in a discriminatory manner, special steps may be required to ensure the system does not unfairly discriminate between individuals or groups of individuals. Furthermore, as noted by CEPEJ, 'the use of machine learning and multidisciplinary scientific analysis to combat such discrimination should be encouraged.'[67]

[66] See further Deeks, A. (2019) 'The Judicial Demand for Explainable Artificial Intelligence'. *Columbia Law Review* 119(7): 1829-1850.

[67] CEPEJ (2018) 'European Ethical Charter' (p. 9).

7.9 The quality assurance principle

Law Ministers may wish to consider and adopt the 'quality assurance principle'. A reliable application of AI systems for judicial decision-making in criminal justice systems must be able to maintain quality assurance and should reliably operate in accordance with its intended purpose, over its lifecycle; while close enough may be good enough in some settings, that is not the case where AI is applied in a criminal justice setting such as in the fight against cybercrime. This places quality and robustness requirements on both the AI system as such and the data it uses. Further, it places quality requirements on the operation of the system by those using it. Certification schemes and external audits, and the involvement of external, independent, expert assessment, may be valuable in this context.

7.10 The resilience principle

While the Commonwealth has already commenced important work on cybersecurity,[68] the world's cyber-dependence has by far outpaced efforts aimed at ensuring cyber-resilience. This has created serious societal vulnerabilities, which are frequently exploited by criminals and hostile state actors. Thus, Law Ministers may wish to consider and adopt the 'resilience principle'. Under this, there should be no situation of full AI dependence. All systems must include back-up features ensuring continuous functionality of the judicial system even where a particular AI system is attacked or otherwise fails. The resilience principle also imposes cybersecurity obligations on users of AI systems, meaning that all reasonable steps must be taken to ensure system integrity, and to avoid manipulation and unlawful access. In this context, users must be mindful that manipulation can take many forms. For example, and also where the algorithms are operating properly, data may have been manipulated either to either cause undue outcomes in a specific instance or to impact the long-term operation of the system.

7.11 The human oversight principle

Many of the risks and challenges identified in Section 5 may be mitigated where the structures adopted include appropriate human oversight,[69] review, audits and intervention. Thus, Law Ministers may wish to consider and adopt a 'human oversight principle' mandating such oversight.

[68] See the Commonwealth Cyber Declaration 2018.

[69] See for example New Zealand Government (2020) 'Algorithm Charter for Aotearoa New Zealand'. Statistics NZ. https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf

7.12 The accountability principle

Law Ministers may wish to consider and adopt the 'accountability principle' that partly overlaps with some of the previously noted principles. The important role accountability can play in technology regulation is widely recognised,[70] and, as outlined by the Australian Human Rights Commission:

> *Accountability involves ensuring that the law is followed in a decision-making process. It includes both a* corrective *function, facilitating a remedy for when someone has been wronged, as well as a* preventive *function, identifying which aspects of a policy or system are working and what needs adjustment.*[71]

7.13 The human-centricity principle

Law Ministers may wish to consider and adopt the 'human-centricity principle' often highlighted in works discussing the regulation and ethics of AI systems.[72] As noted by one such work, 'Put simply, a human-centric approach to AI is placing humans and the human experience at the centre of design considerations and intended outcomes of AI technologies.'[73] Importantly, even where used to pursue legitimate goals such as enhancing the efficiency of tools against cybercrime, the adoption of AI systems for judicial decision-making in criminal justice systems must not undermine human dignity.

7.14 The need for 'red lines'

The above has already alluded to the value of a framework, such as that discussed, containing clear 'red lines' delineating types of AI uses that are incompatible with the values of the Commonwealth member countries. For example, Law Ministers may, as noted, wish to articulate a ban on AI as final arbiter in the context of judicial decision-making in criminal justice systems. Similarly, AI systems' use for general biometric surveillance and for 'social scoring', for example, could be specifically banned.

7.15 Structural arrangements, collaboration, co-ordination and information-sharing

In addition to the framework and principles canvassed above, Law Ministers may wish to explore structural arrangements that support the safe adoption of AI systems for judicial decision-making in criminal justice systems so as to support the fight against cybercrime. For example, the Australian Human Rights Commission has recommended

[70] See for example the work of the Institute for Accountability in the Digital Age: https://i4ada.org/.

[71] Australian Human Rights Commission (2021) *Human Rights & Technology Final Report* (p. 51). See also UNOHCHR (2013) *Who Will be Accountable? Human Rights and the Post-2015 Development Agenda.* HR Pub/13/1, 2013.

[72] See for example Singapore's Model AI Governance Framework (Second Edition) (2020). www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf

[73] AI Asia Pacific Institute (2021) 'Trustworthy Artificial Intelligence' (p. 15).

establishment of an 'AI Safety Commissioner'.[74] The ambit of such a role would include, but also go beyond, the topic of adoption of AI systems for judicial decision-making in criminal justice systems. Law Ministers may wish to consider establishing such a position in their respective countries; where this is done, they may also wish to consider establishing a structure for active collaboration and co-operation between their respective AI Safety Commissioners, perhaps in the form of a Council of Commonwealth AI Safety Commissioners.

More broadly, there are clear benefits to be gained from collaboration, co-ordination, information-sharing, sharing of best practices and support among the Commonwealth member countries in the context of the adoption of AI systems for judicial decision-making in criminal justice systems, cybercrime and AI regulation in general. There is a longstanding recognition that co-operation among Commonwealth member countries is essential in the digital arena,[75] and joining forces may facilitate the policy coherence, joint initiatives and interoperability necessary for interaction among Commonwealth member countries, for example in the context of criminal justice, not least in the context of emerging technologies such as AI and constantly evolving fields such as cybercrime.

Such work can also help address inequality of resources and degrees of development among member countries. In this latter respect, Law Ministers may wish to consider and adopt shared training and training resources, as well as enhanced digital literacy programmes, for example for courts but also for the legal communities more broadly.[76]

7.16 The need for realistic expectations

Where these structures, and the proposed framework with its numerous principles, are adopted, Commonwealth member countries are well placed to enjoy the benefits that AI systems may bring for judicial decision-making in criminal justice systems as a tool to address cybercrime, while at the same time being in a position to manage the risks and challenges involved. Nevertheless, for the foreseeable future, the adoption of AI systems for judicial decision-making in criminal justice systems is likely to provide a support role rather than autonomous decision-making. This is appropriate and discussions must proceed with realistic expectations and an acute awareness of the difference between marketing samples and products ready for safe and compliant, rights-respecting, transparent implementation. Quite a lot of AI is presented as 'almost' perfect, with the

[74] Australian Human Rights Commission (2021) *Human Rights & Technology Final Report* (pp. 127–135).

[75] See the Commonwealth Cyber Declaration 2018.

[76] For example, CEPEJ recommends that 'Generally speaking, when any artificial intelligence-based information system is implemented there should be computer literacy programmes for users and debates involving professionals from the justice system' (CEPEV, 2018, 'European Ethical Charter', p. 12). The emphasis on increasing digital literacy is also found in Commonwealth initiatives such as the Commonwealth Cyber Declaration 2018, stating that 'digital literacy can be a powerful catalyst for economic empowerment and inclusion, and commit to take steps towards expanding digital access and digital inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language.'

promise of perfection around the proverbial corner. However, we must remain alert to the difference between near perfect and actually perfect; progress to the point of near perfection is no guarantee for ever reaching the stage of actual perfection.

Further, there are at least three other considerations that must be flagged briefly so as to at least bring them to the attention of Law Ministers. First, given the centrality of data for the proper operation of AI systems, it is necessary to engage with the supply, quality and protection of the required data. Many countries have started emphasising the value of 'open data' but such arrangements need detailed regulation and thoughtful approaches;[77] at the same time, several countries are adopting 'data localisation' measures.[78] Second, steps must be put in place to address the risk of 'AI systems overreliance' developing in judicial decision-making. Law Ministers may wish to consider and adopt specific administrative tools for monitoring and eliminating such overreliance. Third, Law Ministers may wish to consider and adopt steps aimed at avoiding oversimplification of the law stemming from pressures to make it easier for AI systems to work with the law. Put simply, law is painted with all the colours of the spectrum and, while legal certainty and clarity are valuable goals, we must avoid making the law black and white just to cater to machines applying it.

7.17 Recalling the difference between 'can' and 'should'

In the end, there are two overarching key questions with which Law Ministers must engage. The first is whether AI systems *can* play a role in judicial decision-making in criminal justice systems to address cybercrime. Engaging with this question requires account to be taken of matters such as technical limitations (including limitations imposed by the extent to which law in general – as opposed to specific aspects of law – can be reduced into code), compliance limitations (including the extent to which our current law caters to AI systems playing a role) and the constantly developing AI technology. It is also necessary to consider the complex relationship between technology and law. For example, if benefits may be gained from AI systems without undermining fundamental values, there may be instances where laws and procedures could be amended to better accommodate such AI systems. In other words, law and technology must be approached as a system.

The second question is whether AI systems *should* play a role in judicial decision-making in criminal justice systems to address cybercrime. This is the more important question, and it is a question that benefits from multistakeholder input and public debate.

[77] See further: Gloria Gonzalez Fuster, G. (2020) 'Artificial Intelligence and Law Enforcement' - Impact on Fundamental Rights, (July 2020) https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf, at (pp. 28-–29).

[78] See further Svantesson, D. (2020) 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines'. Digital Economy Paper 301. Paris: OECD.

While obviously related, the 'can' question and the 'should' question are best approached separately. Failure to do so would create a risk that the answer to the question of whether AI *should* play a role in judicial decision-making in criminal justice systems to address cybercrime is overshadowed by the excitement and hype often associated with the question of whether AI *can* play such a role.

The Commonwealth Cybercrime Journal

Print ISSN 2959-3018, online ISSN 2959-3026

Disclaimer

The Commonwealth Secretariat makes every effort to ensure the accuracy of all the information (the 'Content') contained in our publication. However, the Commonwealth Secretariat makes no representations or warranties whatsoever as to the accuracy, completeness or suitability for any purposes of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors and are not the views of or endorsed by the Commonwealth Secretariat. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. The Commonwealth Secretariat shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

Printed copies

A small number of printed copies of the journal are produced and distributed by the Commonwealth Secretariat on a not-for-profit basis. No formal sales or distribution arrangements for the journal are currently in place. To register your interest in receiving a printed copy of this and/or future issues of the journal please contact n.amobi@commonwealth.int or cybercrime@commonwealth.int.

The Commonwealth

Contents

D19156