The Commonwealth

Commonwealth Cybercrime Journal \ 1
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.

Brain 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.