Commonwealth Cyber Journal \ 1
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Editorial

Nkechi Amobi and Aidan Ferguson

The security and trustworthiness of internet infrastructure is essential in today's society. Cybersecurity research has, therefore, taken inspiration from a wide range of fields to accomplish this goal. This research has involved the implementation of various measures to ensure the confidentiality, integrity and availability of digital assets. Yet, these cybersecurity initiatives must also now navigate the challenges posed by artificial intelligence (AI).

AI is the fastest growing deep technology[1] in the world, and its use has the potential to rewrite the operational and policy rules of governments and industries. AI is becoming ubiquitous and has the potential to drive substantial global economic growth by replacing or becoming a viable alternative to human endeavours. However, as AI's benefits rapidly grow, so do its risks.

AI and cybersecurity have a complex relationship. On one hand, AI techniques can be leveraged to enhance cybersecurity measures by detecting and responding to threats more efficiently than traditional methods. Yet AI also introduces new cybersecurity risks. As AI systems become more advanced and integrated into critical infrastructures, they become potential targets for adversaries seeking to exploit vulnerabilities or manipulate their decision-making processes. While it is essential to recognise the risks posed by AI, nations must seize the substantial opportunities that it presents to build various aspects of their economy, including cybersecurity and resilience – ideals recognised in the 2018 Commonwealth Cybercrime Declaration.[2]

In 2023 the Commonwealth Secretariat established the Commonwealth Artificial Intelligence Consortium (CAIC) with the aim of leveraging AI's potential to empower citizens – especially women and girls, youth and other vulnerable groups – with the necessary skills to benefit from the opportunities to be found in cyberspace. Through the creation of AI education and skills courses, the development of AI and related digital infrastructure, responsible AI policies and regulations, and capacity-building initiatives on AI safety, the CAIC has promoted capacity-building throughout the Commonwealth through its working group. Furthermore, at the 2024 Commonwealth Law Ministers Meeting, held in Zanzibar, the development of a comprehensive approach that integrates AI and virtual technologies to assist citizens in accessing justice across the Commonwealth was endorsed by Law Ministers in recognition of the interplay between AI and the justice system.

[1] Office for Artificial Intelligence (UK) (2021, September) National AI Strategy. Command Paper 525. London. Available at: https://www.gov.uk/government/publications/national-ai-strategy

[2] See https://thecommonwealth.org/commonwealth-cyber-declaration-2018

The *Commonwealth Cyber Journal* (*CCJ*), published by the Commonwealth Secretariat, serves as a platform for disseminating cutting-edge research, policy influencing articles, case studies and commentary from practitioners, policy-makers and academics in the field of cybersecurity and cybercrime. The objective of the *CCJ* is to assist Commonwealth countries to strengthen their anti-cybercrime legislative, policy, institutional and multilateral frameworks to uphold the rule of law in both virtual and physical spaces.

In the special section on artificial intelligence

This second edition of the *CCJ* primarily focuses on AI: its first five articles, collected together in the special section on AI, address emerging threats and employ AI approaches to improve cybersecurity safeguards. The contributors to this issue cover topics including AI in the justice system; generative artificial intelligence-led crime as a service (GAI-led CaaS); violent extremists and AI; AI and the future of intellectual property rights; analysis of the Budapest Convention and draft UN anti-cybercrime framework; and the future of cyber insurance and cybercrime in the Asia-Pacific region.

Olalekan Bello and Cecile Ogufere's article on 'The Emerging Artificial Intelligence Legal-Judicial Systems' Interface: Assessing the State of Nigeria's Judicial System's Readiness for a Revolution' analyses how AI is revolutionising various sectors, including the legal-judicial system. Their article highlights how AI can be used to predict case outcomes, streamline contract review processes, save time and resources for legal professionals and assist judges in making more informed decisions. Despite its potential benefits, the article notes that Nigeria's judicial system faces numerous challenges that may hinder its readiness for an AI revolution. Their paper focuses on how that system can draw insights from the emerging global frameworks to establish its own regulations to implement AI technologies, safeguard the rights of citizens and ensure fair and unbiased decision-making processes. The article discusses the opportunities and challenges of integrating AI into Nigeria's judicial system, and concludes that by addressing existing barriers and establishing robust ethical and legal frameworks, the legal-judicial system can harness the potential of AI to enhance efficiency and decision-making processes.

Nicole Matejic and Chris Wilson, in their article 'Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service', advance the idea that crimes of influence are crimes that seek to influence people towards harmful outcomes, and will be a defining feature of generative AI-led cybercrime. While the technology itself is a regular feature of contemporary discussion and research, less thought has been given to the ways in which generative AI (GAI) impacts human cognition to create increasingly permissive environments in which cybercriminals and terrorists can operate. Their paper explores how GAI will likely evolve to deliver persuasive influence at potentially unavoidable economies of scale, while also considering current Commonwealth and global governmental and multistakeholder responses to these challenges.

Gilberto Martins de Almeida, Fernando Bourguy, João Farrel and Diego Semeraro, in their article 'Legal application of technical and procedural standards and frameworks in the combat against GAI-powered cybercrime', acknowledge that GAI has deepened the gap between fast-changing innovative cyberattacks and the slow pace of legislative processes. In the article, the authors argue that to mitigate the resultant exposure, states should look for ways to address this gap. One option to be considered is resorting to standards, which may provide faster adoption, more specific focuses and international recognition. They note that this is particularly valid for the Commonwealth's small states, whose structures may not be as resourceful as those of larger states. In this sense, they posit that standards could be used to fill in the blanks of cybercrime laws (such as indicating that GAI could fall within the concept of 'computer system', which already exists in the cyberlaws of many Commonwealth small states). In summary, the article analyses the convenience of building effective supplementation and constant updates by and between standards and legal rules, referring to several published standards which could be helpful for the prevention of GAI-powered cybercrime.

Wan Rosalili Wan Rosli's article, 'Violent Extremism and Artificial Intelligence: A Double-Edged Sword in the Context of ASEAN', advances the argument that cyberspace has created a new haven from which terrorist organisations can carry out terrorist activities, which has resulted in unprecedented transnational extremism and extremist networking. The emergence of new technologies such as AI has also provided a new sandbox in which insurgents can spread their propaganda. The article provides a discussion on the duality effect of AI in countering violent extremism within ASEAN by highlighting the risks and vulnerabilities attached to the deployment of such technologies, and sheds light on both how such technologies can be misused and how ASEAN states can respond to the risks associated with AI.

Teresia Munywoki's article 'AI Systems and the Future of Intellectual Property Regimes' explores the relationship between AI and intellectual property rights (IPR), highlighting the challenges and opportunities that arise from their intersection. She posits that, given AI's pervasive influence across various sectors, questions surrounding authorship, ownership and protection of AI-generated innovations have emerged. She argues that traditional IPR frameworks, designed with human creators in mind, now face the task of adapting to accommodate the unique characteristics of AI-generated content and inventions. The discussion spans patent law, copyright issues and ethical issues, highlighting the need for a balanced approach that fosters innovation while safeguarding the rights of all stakeholders. The legal dilemmas that Munywoki highlights, such as determining inventorship for AI-generated inventions and attributing copyright for AI-created content, underscore the complexity of this evolving landscape. Her article also emphasises the importance of collaborative efforts to shape a future-proof IPR framework that balances innovation, accessibility and ethical considerations in the AI era.

Also in this issue

Eric Cho and Serene Chan, in the article 'Ensuring a Secure Future by Insuring Against Cybercrime', argue that with rapid advancements in technology and digitalisation, cybercrime has emerged as a formidable threat capable of disrupting business operations and causing financial impacts across society. They note that for years, insurance has become a method of transferring such risks from businesses and individuals to third-party entities, offering a sense of reassurance and protection. With this emerging risk, there is a compelling case for the utility of insurance in addressing this need for risk transfer in the market. Beyond this mitigating solution, the authors also underscore the importance of government intervention, emphasising cybersecurity as a matter of national security. Acknowledging the limitations of the private insurance sector, the authors advocate for collaborative efforts between public and private entities to address the multifaceted challenges posed by cyber risks in effective ways.

In his paper, 'The National Security Exception in International Trade and Cybersecurity', **Kartikeya Garg** theorises that international trade and cybersecurity are becoming increasingly interconnected, with countries implementing various digital technologies to facilitate cross-border trade in goods, services and information. To regulate this, countries could adopt various cybersecurity policies such as data localisation, export controls and import restrictions; however, these may be trade-restrictive and violate World Trade Organisation (WTO) law. Garg argues that the national security exception contained in WTO agreements, and most free trade agreements (FTAs), provide countries with an avenue to escape certain multilateral trade obligations. Historically used for protection against traditional security attacks, this article discusses the evolution of the national security exception within the WTO and other FTAs to determine whether existing treaty formulations can extend to cybersecurity measures. The paper recommends formulations and considerations that countries could implement to create a more holistic security exception in the international trade regime.

Olajide O. Oyadeyi, Oluwadamilola Adeola Oyadeyi and Rofiat Omolola Bello, in 'Cybercrime in the Asia-Pacific Region: A Case Study of Commonwealth APAC Countries', advance the theory that the digital transformation in the Asia-Pacific (APAC) region, coupled with its expanding economic activities and online presence, has made it a prime target for cybercrime. They note that according to cybercrime projections, the region faces a potential cost of roughly US$3.3 trillion from cybercrime by 2025. The authors discuss the context behind cybercrime in the APAC region, particularly its post-COVID proliferation; the pros and cons of the potential use of AI in cybersecurity; cybersecurity initiatives and strategies in the Commonwealth APAC region; and options for policy consideration.

Finally, **Brenda Mwale**'s article 'Towards a Victim-Centred Approach? Reflections on Existing Cybercrime Instruments and the Draft United Nations Convention on Cybercrime' advances the argument that punishing offenders through a retributive approach is often not sufficient to address the plight of victims of cybercrime, given the unique impact that such crimes can have. Having examined the extent to which existing cybercrime instruments, and the draft UN Convention on Cybercrime, address victims' needs, Mwale argues that legal approaches to addressing cybercrime should adopt a victim-centred approach that offers them adequate safeguards to protect them, and human rights guarantees.