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

Editorial

Nkechi Amobi

The Commonwealth Secretariat, sponsored by the UK government, continues to undertake numerous capacity-building initiatives to enhance the cyber resilience of its member countries through collaboration and innovative practices.

As the digital landscape continues to evolve at a staggering pace, the *Commonwealth Cyber Journal* provides a vital platform to explore the pressing cyber challenges and opportunities facing nations across our shared community. Technological innovation offers remarkable opportunities and undoubtedly makes our lives more convenient and our society more efficient, but these changes also bring with them exposure to issues in the areas of security. As the Commonwealth continues to embrace the possibilities of the digital age, we are confronted with complex and evolving cyber threats that transcend borders.

This edition of the *Commonwealth Cyber Journal* brings to the forefront key issues that demand our collective attention and action. We are proud to present articles offering insights and practical approaches to protecting critical information infrastructure, an area of growing concern as essential services and national assets increasingly rely on interconnected systems. Lessons shared in this edition highlight the vulnerabilities of member countries and the innovative strategies being deployed to secure these vital sectors. As digital platforms become arenas for harassment, coercion, and harm, the need for a coordinated response rooted in human rights and gender-sensitive approaches becomes more paramount. The contributions in this issue challenge us to consider how cyber policies practices and guidelines may better protect the most vulnerable among us.

This volume assesses how honeypots are becoming increasingly valuable tools in understanding and mitigating cyber threats. Exploring this technique within the Commonwealth context offers practical guidance and broader reflections on proactive cybersecurity measures. As a diverse family of nations, we have much to learn from one another, and the *Commonwealth Cyber Journal* remains committed to amplifying these conversations. We encourage all readers— policymakers, practitioners, researchers, and the public—to engage with the ideas presented in this edition and consider how they may be applied within their contexts. Cybersecurity is not solely a technical issue but a matter of national resilience, human security, and collective responsibility.

As we look ahead, let us reaffirm our shared commitment to a secure, open, and inclusive cyberspace for the benefit of all Commonwealth citizens.

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 this issue

In this third issue of the *Commonwealth Cyber Journal (CCJ)*, contributors explore a range of important topics. These include the use of Advanced Cyber Defence (ACD) by private corporations to safeguard their operational data and that of their customers. The issue also addresses the effectiveness of current laws and regulations in preventing cybercrime and protecting personal information within the Commonwealth.

Other articles in this volume explore international legal frameworks for combating Online Child Sexual Exploitation and Abuse (OCSEA) and compare them with existing legal systems in the MENA region. Additionally, contributors examine the global challenge of cybersecurity in smart grids from the perspectives of several Commonwealth countries, and national cybersecurity frameworks.

Furthermore, the issue examines the connection between cybercrime and online gambling, as well as legislation targeting cyberstalking and technology-facilitated intimate cyberviolence.

In *The Use and Legality of Honey Pots, Tracers, and Trackers in Australia*, **Brendan Walker-Munro et al**. tackle an important topic in cybersecurity today. As cyber attackers—state-sponsored, criminal, or opportunistic—become increasingly sophisticated, the role of proactive defence mechanisms like ACD comes to the forefront. This paper introduces the most common forms of ACD, including decoy assets and tracking technologies, and examines the significant legal, ethical, and regulatory dilemmas associated with their use. Through a focus on Commonwealth jurisdictions, notably Australia, the authors propose much-needed legal reforms to enable ACD as a legitimate tool for private sector resilience—an important contribution to ongoing global cybersecurity policy and law debates.

In his article, *Strengthening Cybersecurity and Data Protection Frameworks in Commonwealth Member Countries: Policy and Institutional Approaches*, **Otshepeng Mazibuko** examines how Commonwealth countries are addressing the gaps in safeguarding personal information. The article assesses the unevenness in current regulatory frameworks and international cooperation in a world where data flows seamlessly across borders. Highlighting key issues such as cybersecurity capacity building, cross-border data sharing, and digital sovereignty, Mazibuko calls for a renewed

commitment to international collaboration that balances local needs and realities. This is an essential roadmap for Commonwealth countries seeking to strengthen their cyber resilience while respecting individual rights.

Mohamed Hemdani's piece, *Cyberstalking and Intimate Partner Violence: How Technology Escalates Abuse (OCSEA)*, offers a comparative analysis of international and MENA regional legal frameworks. By examining jurisdictions such as Egypt, Saudi Arabia, and the UAE and comparing them with systems like the United Kingdom, Hemdani reveals critical gaps and cultural complexities in addressing OCSEA. Given the global nature of these crimes and the vulnerabilities they exploit, his call for harmonised, culturally sensitive, and enforceable legal frameworks is both timely and urgent.

The article *Cybersecurity Threats to Critical Energy Infrastructure: Challenges and Opportunities for Developing Nations*, written by **Rohini Haridas et al.,** focuses on a critical yet underexamined area: energy infrastructure. As nations embrace the benefits of smart grids, the vulnerabilities inherent in these interconnected systems grow. Drawing on the case of India, this paper highlights the specific challenges developing countries face—limited resources, policy gaps, and the accelerating digitisation of critical infrastructure. The analysis highlights the need for comprehensive security frameworks that can keep pace with the rapidly evolving threat landscape of energy systems.

Focusing on Nigeria, **Samuel Iheanyi Nwankwo**, in his paper *Strengthening Nigeria's Cyber Frontier: Building Resilience Through Legal Innovation*, addresses the urgent need for a modernised cybersecurity framework in one of Africa's largest economies. Through a detailed examination of Nigeria's fragmented and outdated legal and institutional landscape, Nwankwo proposes a "resilience-based blueprint"—a forward-looking approach that integrates preparedness, adaptability, and recovery into national cybersecurity efforts. His recommendations for proactive legislation, robust incident response, and capacity building provide an actionable pathway to enhancing Nigeria's—and, by extension, similar jurisdictions'—cybersecurity posture.

From the African continent to South Asia, **Md Masudul Islam Khan** et al. highlight *The Nexus between Cybercrime, Financial Fraud, and Online Gambling in Bangladesh*. Their research examines how illicit online gambling platforms could facilitate money laundering and fraud, exploiting gaps in regulation and enforcement. By shedding light on how social media, digital payment systems, and bureaucratic inertia contribute to this growing problem, the authors advocate for urgent legislative reforms and improved cross-border cooperation to tackle these emerging cyber-financial crimes.

Chioma Aneh's article, *Cyberstalking and Intimate Partner Violence: How Technology Escalates Abuse*, explores cyberstalking as a form of technology-facilitated intimate partner violence (TFIPV) in Nigeria, Kenya, and South Africa. It examines how digital tools, such as spyware and social media surveillance, are used against victims, highlighting legal gaps and inadequate support systems. Despite global frameworks like the Budapest Convention, African responses remain fragmented. The study advocates for

harmonising laws, improving law enforcement training, enhancing digital literacy, and holding tech companies accountable while emphasising survivor-centred approaches in cybercrime strategies.

Together, these contributions reflect the diversity of cyber challenges confronting Commonwealth nations—spanning advanced industrial economies and emerging markets alike. The *Commonwealth Cyber Journal* remains committed to fostering dialogue, research, and action that bridge legal, policy, and technical domains, recognising that cyber threats are as varied as they are complex.