The Commonwealth

Commonwealth Cyber Journal \ 79
Print ISSN 2959-3018, online ISSN 2959-3026
thecommonwealth.org/Cyber-journal

Strengthening Cybersecurity and Data Protection Frameworks in Commonwealth Member Countries: Policy and Institutional Approaches

Otshepeng Mazibuko[1]

Abstract

In an increasingly interconnected world, cyber threats pose significant risks to the security and privacy of individuals, organisations and governments. As digital ecosystems expand, the legal, policy and institutional frameworks governing cybercrime and cybersecurity must evolve to ensure the protection of personal data and the privacy of users. This paper explores the current state of privacy and data protection mechanisms within Commonwealth countries, highlighting the disparities, challenges and opportunities in developing more effective frameworks. Drawing on recent trends, this paper examines the effectiveness of existing legislation, policy and initiatives designed to combat cybercrime and improve data protection. It also investigates how different Commonwealth countries address issues such as cross-border data sharing, cybersecurity capacity building and digital sovereignty. It gives special attention to the role of international co-operation and institutional development in mitigating emerging cyber threats and fostering a resilient cybersecurity environment across the Commonwealth. By assessing both successes and gaps, the paper proposes strategies for strengthening data protection laws, improving cybersecurity infrastructures and fostering multilateral partnerships that can promote a secure digital landscape. It aims to contribute to the ongoing discourse on privacy and cybercrime governance and offer policy recommendations that Commonwealth nations can implement to safeguard their digital future.

1 Research assistant at the University of Cape Town for a PUBGEM-Africa project, GeneMAP Research Center, and PhD candidate at the University of Pretoria.

1. Introduction

As the world is being digitalised, governments, organisations and individuals are concerned with critical issues of cybersecurity and data protection (Shackelford 2012). These concerns relate to the sensitive data generated, processed and stored together with the speed, complexity and volume of digitalisation (Clarke 2019). This technological development contributes to socio-economic growth, but the associated data breaches, cyber-attacks and privacy violations pose significant risks (Smith et al, 2020).

Challenges with cybersecurity and data protection persist. This relates to the variation in levels of economic development and technological adoption across the Commonwealth. This needs to be addressed by the Commonwealth (Commonwealth Secretariat, 2018). Some countries are struggling with resource constraints, fragmented regulatory frameworks and gaps in capacity. These prevent them from fulfilling their role in implementing data protection measures (Arora and Luthra 2021). However, cultural similarities, historical ties and collaboration bring opportunities for confronting the challenges – not in silos, but collectively (Weber 2020).

This paper examines differences in data protection procedures and cybersecurity preparedness in Commonwealth nations. It considers difficulties for countries in protecting privacy and personal information and suggests areas for co-operation, capacity building and policy harmonisation (Mistry 2022). It aims to add to continuing discussion on improving cybersecurity and data protection in the Commonwealth context by pointing out gaps and suggesting workable solutions.

2. The cybersecurity landscape in Commonwealth countries

Groups of nations that form the Commonwealth have undergone different levels of digital transformation. Advanced economies have enhanced their digital infrastructures and broadened coverage. (Commonwealth Telecommunications Organisation 2019). Although these advancements showcase the association's strengths and capabilities, they also highlight the challenges posed by cyber threats. This is evident in developed countries such as Canada and the United Kingdom through their well-designed cybersecurity frameworks (Johnson 2017).

The threats are significant because Commonwealth nations are diverse. Individuals and organisations face identity and intellectual property theft, which compromise them greatly (Sharma 2020). Hackers disguise themselves as sophisticated and state-sponsored to directly attack critical infrastructure including power grids, healthcare systems and financial institutions (Clarke 2019). Threats are compounded for member countries with inadequate resources to enforce regulations, or where there is less co-operation with others (Mistry 2022).

Privacy and data protection measures are essential for combatting cyber threats. Cybersecurity needs strengthened more broadly to protect individuals' data and to enhance trust in digital systems (Sharma 2020). Sensitive information must be protected through effective data protection measures to eliminate cyber-attacks (Weber 2020). Geopolitics and socio-economic disparities make it difficult for the Commonwealth to adopt uniform standards for data privacy (Arora and Luthra 2021).

3. Legal, policy and institutional frameworks

Commonwealth nations have differences and similarities, for example legislation, socio-economic contexts and technologies. These shape the associations' legal framework for governance in privacy and data protection (Commonwealth Secretariat, 2018a; Greenleaf 2021). Some of the developing and underdeveloped countries lack privacy legislation and the capacity to update legal frameworks as needed. In comparison, the UK has data protection laws that align with the European standards of the General Data Protection Regulation (GDPR) (ICO 2021).

The advantages of comprehensive legal protection are evident in nations with highly developed regulatory frameworks. Accountability and the rights of individuals, particularly the rights to access and to ensure the accuracy of their data, are embedded in the UK's Data Protection Act 2018, which assures personal data protection. Guidelines stipulated in Australia's Privacy Act 1988 place restrictions on cross-border data transfers and on the handling of personal information.

However, it is difficult for many developing Commonwealth nations to set up and implement comparable systems. The non-existence of comprehensive legal provisions makes them vulnerable to data misuse and cybercrime. Nevertheless, countries such as Kenya and Nigeria have enacted data protection laws consistent with global good practice, indicating progress (DataGuidance 2020; OAIC 2020). Data Protection Act principles such as data minimisation, consent-based processing and accountability, are reflected in the Kenyan framework, which aligns with global practice and standards.

Despite such developments there are challenges with the implementation process, and inconsistencies in the scope and enforcement of any legislation. This hinders effective partnership and cross-border data sharing across the Commonwealth (Commonwealth Secretariat ,2018b). Co-ordination and legal assistance are needed across Commonwealth member countries to improve transnational cyber threats.

Assessment of institutional frameworks for cybersecurity

Institutional frameworks need to be efficient to ensure the implementation and enforcement of established legal provisions. Such frameworks vary across the Commonwealth. Developed and resourced countries such as the UK and Singapore have established regulatory bodies such as the Information Commissioner's Office (ICO)

in the former and the Personal Data Protection Commission (PDPC) in the latter. This enables handling of intricate issues, including compliance campaigns, public education and awareness campaigns, and data breaches (ICO 2021; PDPC 2022).

Under-resourced countries lack the institutional capacity to implement and enforce privacy and cybersecurity laws effectively. It means that agencies struggle with fragmented governance, limited technical expertise, mandates that overlap and inadequate funding (Greenleaf 2021). For example, the enforcement of existing laws and public trust in digital systems are undermined by the non-existence of data protection authorities in some of the African Commonwealth nations.

Capacity-building initiatives and regional cooperation can help address this challenge. Programmes like the Commonwealth Cyber Programme offer training and technical assistance to member countries. Additionally, international organisations such as the International Telecommunication Union (ITU) can enhance the capabilities of under-resourced institutions (ITU 2021).

Gaps and inconsistencies in legal and policy measures across member countries

A coherent and integrated strategy for cybersecurity and data protection is made extremely difficult by the Commonwealth's disparate legal and policy frameworks. These disparities show themselves in several ways including:

1. Scope and coverage

The absence of comprehensive privacy laws and the reliance on sector-specific regulations mean that countries fail to confront the implications of data protection in the digital economy. Critical sectors such as healthcare and education are prone to cyber threats due to segmented approaches (UNCTAD 2021).

2. Enforcement mechanisms

For privacy and cybersecurity to be effective, adequate authority, resources and regulatory bodies are needed. Low compliance and limited-to-no accountability for violations in many Commonwealth countries result from weak or non-existent enforcement mechanisms (Greenleaf, 2021).

3. Cross-border data transfers

Complex international partnerships and inconsistent policies on cross-border data transfers create legal uncertainty for businesses operating across multiple jurisdictions (ICO 2021; OAIC 2020). While some countries lack a data protection framework, others, like Australia and the UK, have established clear guidelines

4. Public awareness and education

Public education and education campaigns enable legal and policy measures to be effective. In many Commonwealth nations legislative efforts are weakened by their citizens' lack of knowledge about privacy and cybersecurity risks (PDPC 2022).

Confronting these gaps requires an organised approach that emphasises the harmonisation of laws; encourages and promotes public-private collaborations; and builds capacity. Challenges could be overcome by leveraging the expertise and resources of Commonwealth member countries and establishing a solid legal and institutional framework for data protection, including protection of personal data.

4. Challenges in cybersecurity and data protection

Cross-border data sharing: Issues and implications for privacy

Data needs to be able to flow across borders to enhance and develop the commercial, innovation and governance sectors. But there are challenges because of the different legal systems and data protection levels across Commonwealth countries (Daly 2020). Different privacy regulations and frameworks may lead to a lack of trust within shared digital ecosystems (Greenleaf, 2021).

There may be a lack of clarity about data ownership and jurisdiction. The individual responsible for safeguarding data, particularly in transnational systems prone to breaches, raises critical concerns about safety and security (ITU 2022). Moreover, unresolved issues related to surveillance and the misuse of personal information can hinder partnerships and the establishment of international collaboration. A coherent approach to respecting national laws and building trust in shared systems can help to overcome concerns (Commonwealth Secretariat 2018c).

Data localisation policies for ensuring that countries' data do not move beyond borders vary considerably. While such policies are supposed to protect data subjects or citizens in general, they can prevent economic integration and can lead to conflict (Greenleaf 2021). This hinders access to global markets and technological advancement.

Cybersecurity capacity building: Barriers to implementation in resource-constrained countries

Effective data protection and privacy requires sustained capacity building to strengthen cybersecurity. Under-resourced Commonwealth countries with a lack of transferable skills, policies and practical infrastructure to confront cyber threats, face barriers in ensuring regulation (ITU 2022).

Lack of finance is a major barrier to investing in training, adapting technology, and developing and maintaining concrete cybersecurity systems. For developing countries in the Commonwealth, immediate priorities, such as healthcare, education and poverty alleviation, must compete with such investment (Commonwealth Secretariat 2018b).

Lack of professional expertise is another obstacle. Mobility and migration of skilled personnel for career opportunities elsewhere, lead to a lack of qualified staff in the highly specialised field of cybersecurity in some countries. Low- and middle-income countries (LMICs) run the risk of being unable to detect and effectively respond to cyber threats because of the lack of local expertise (Daly 2020).

Capacity-building initiatives are delayed by institutional weakness. Commonwealth nations often lack committed cybersecurity agencies to drive national efforts through clear policy frameworks and regulations. In some instances, the intervention and involvement of politics and bureaucracy aggravates this, raising questions of sustainability (ITU 2022).

Digital sovereignty: Balancing national interests with global co-operation

As an association of member countries, the Commonwealth faces growing challenges in managing data governance, as this is perceived to undermine the digital sovereignty of individual member countries. This tension is contributing to resistance towards global collaboration on cybersecurity and data protection (Greenleaf 2021).

It can be difficult to find a balance. Controlling digital resources is important for protecting the privacy of citizens. Isolationist policies limit access to global expertise exposing countries to cyber threats that go beyond borders.

Some Commonwealth nations safeguard their sovereignty by implementing policies that restrict internet governance. This is to control internal cyberspace. However, this limits international partnerships and economic growth and suppresses innovation (Daly 2020). To address this tension and promote meaningful participation in global cybersecurity efforts, the frameworks enable countries to assert control over their digital sovereignty.

Community-based training programmes

To close the digital literacy gap, community-based training initiatives in some member countries, use the expertise of nearby NGOs and civic leaders. To make training inclusive and accessible, these initiatives provide interactive workshops in regional languages. By emphasising practical skills including smartphone use, online service access and basic troubleshooting, such training guarantees that participants acquire real-world digital competence. Influencers in the community can act as advocates for digital literacy, boosting long-term involvement and programme participation. Furthermore, modifying

the training to meet community needs – like expanding access to healthcare or putting farmers in touch with agricultural markets – guarantees that such training initiatives have a significant and long-lasting effect.

Educational and public-private partnerships

Collaborating with educational institutions provides a long-term strategy for promoting digital literacy from a young age. Consistent exposure to critical abilities is ensured by incorporating digital skills into the standard curriculum at all educational levels. In order to encourage students to use digital technologies to tackle real-world problems, educational institutions can also offer seminars, coding camps and hackathons. Programmes for training teachers are essential for giving them the skills they need to teach digital knowledge. Educational institutions can give students access to resources like computers, internet connectivity, internships and mentorship opportunities. Partnerships with the private sector may strengthen these initiatives and close the gap between education and real-world application.

Public awareness campaigns

Campaigns to raise public awareness are essential for advancing cybersecurity and digital literacy and for encouraging safer online conduct in all communities. Social media platforms can provide interesting content like infographics, videos and interactive posts that appeal especially to younger audiences. Important messages about internet safety can be amplified through partnerships with thought leaders, celebrities or local influencers. Town hall talks and digital literacy fairs are examples of community events that provide attendees with the chance to speak with professionals face-to-face and to learn about cybersecurity best practice. The significance of such campaigns is demonstrated by successful examples such as the 'Stay Safe Online' campaign- https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2024-05/cybercrime_laws_updf.pdf?utm_source=chatgpt.com, that raises awareness of phishing scams, data protection and secure password practice in effective and relatable ways.

5. Role of multilateral co-operation

Examination of existing Commonwealth-wide initiatives and partnerships

A multifaceted partnership is essential in addressing and combating challenges related to data protection and cybersecurity within the Commonwealth. This is to facilitate meaningful collaboration, capacity building and knowledge sharing among member countries.

An important milestone in promoting cybersecurity resilience is the adoption of the Commonwealth Cyber Declaration in 2018. It emphasises capacity building, the protection of critical infrastructure and the importance of international co-operation. It recommends that Commonwealth member countries integrate the framework to align effectively with global cybersecurity standards.

There are other programmes, such as those offered by the Commonwealth Telecommunications Organisation (CTO), aimed at supporting member countries to improve and confront information and communication technology (ICT) capabilities and cybersecurity challenges. These include workshops, training sessions and guidance through policy processes, essential for establishing and promoting best practice across the Commonwealth.

These programmes highlight the necessity for collective action and for adoption of stronger institutional mechanisms to enhance effectiveness. Member countries continue to face the challenges that these programmes aim to address. This emphasises the importance of sustained support and accountability.

Importance of international collaboration in combatting cybercrime

International collaboration is effective in addressing and combatting cybersecurity challenges globally. This is particularly important to Commonwealth member countries as they share vulnerabilities to cyber threats that are of significant concern.

The investigation and prosecution of cybercrime are key areas in which international collaboration can provide a collective response. Cyber hackers exploit regulatory loopholes and legal gaps to evade accountability. Mutual legal assistance treaties (MLATs) are collaborative frameworks that enable countries to share intelligence, pursue justice and co-ordinate investigations through joint taskforces.

Global partnership promotes the exchange of best practice and recommendations on technological advances. This enables member countries to enhance their access to cutting-edge solutions for combatting cyber threats through international forums and collaborative working groups. The joint approach fosters trust and solidarity in the collective response to emerging challenges.

Best practice from successful initiatives

Numerous approaches strengthen joint partnerships within the Commonwealth by providing valuable lessons. For example, the Malabo Convention is a formal regional framework of the African Union that co-ordinates cybersecurity and data protection initiatives. The regional model consistently demonstrates the ability of regional agreements to align policy and foster collective action.

The European Union's GDPR has paved the way for, and shaped, global privacy legislation. Compatibility and greater integration are key principles of GDPR that help Commonwealth member countries strengthen their respective data protection frameworks.

Platforms that promote knowledge transfer and skills development have proven to be effective in enhancing capacity and fostering innovation. For example, a balanced and resilient cybersecurity ecosystem could be achieved by pairing developed countries with under-resourced ones, effectively transferring skills and technologies.

6. Opportunities for strengthening frameworks

Recommendations for enhancing data protection laws and policies

Commonwealth nations should strengthen their respective data protection laws and policies while recognising the distinct legal and socio-economic contexts of each member state. Data protection must have an established baseline, drawing lessons from the GDPR (European Union 2016). Core principles such as data minimisation, transparency and accountability can serve as a framework for Commonwealth nations to adopt incremental approaches towards an equivalent system.

Commonwealth countries should prioritise establishing independent data protection authorities and commissioners, equipped with context-specific regulations and enforcement mechanisms to ensure compliance. Such authorities can provide guidance on best practice, investigate breaches and impose penalties.

Maintaining contextual relevance, along with stakeholder involvement and public engagement, can effectively facilitate the policymaking process. The practice of inclusivity can address concerns about the rights of marginalised communities in the context of emerging data-driven technologies, such as artificial intelligence (AI), and its effects on small businesses.

Strategies for building resilient cybersecurity infrastructures

Technology, policy and human resources must all be used in a complex strategy to create resilient cybersecurity infrastructures. Prioritising the creation of national cybersecurity policies that address regional risks and conform to international standards should be a top priority. Protecting critical infrastructure requires significant investment. Adopting cutting-edge technologies like multi-factor authentication, intrusion detection systems and zero-trust architectures is part of this. Since the private sector frequently controls sizeable portions of vital infrastructure, public-private partnerships can be extremely important.

Building capacity is equally important. To resolve the global scarcity of qualified cybersecurity specialists, governments must invest in education and training. Local talent pools can be developed with the aid of initiatives like public awareness campaigns,

specialised training programmes and scholarships. Mechanisms for incident response and recovery ought to be improved too. Establishing computer emergency response teams (CERTs) or security operations centres (SOCs) can enable nations to detect, respond to and mitigate cyber threats effectively.

Approaches to foster multilateral partnerships and knowledge sharing

Because cyber threats are transnational, multilateral collaborations are essential. The Commonwealth provides a special setting for encouraging these kinds of partnerships. Establishing regional centres for cybersecurity research and innovation is one strategy that uses the resources and experience of developed member countries to assist others. Knowledge-sharing platforms, like the programmes of the CTO, can help spread technical know-how, case studies and best practice. Regular workshops, online training courses and co-operative projects involving various stakeholders should all be added to these platforms.

Harmonising legal frameworks to facilitate smooth cross-border co-operation should be another goal. This entails establishing MLATs, co-ordinating data protection standards and developing procedures for co-operative cybercrime investigations. Commonwealth nations intending to improve their cybersecurity capabilities can benefit from additional resources and knowledge offered by international organisations such as the ITU and INTERPOL.

7. Case studies

Analysis of selected Commonwealth countries

Analysing the methods used by different Commonwealth nations indicates a range of approaches to and results from data protection and cybersecurity.

UK

With reputable frameworks like the Government Cyber Security Strategy, the UK is a leader in cybersecurity. Establishing the National Cyber Security Centre (NCSC) has improved the country's capacity to identify and address threats. Strong privacy rights are guaranteed under the UK's Data Protection Act 2018, which includes the GDPR. The significance of institutional leadership, consistent infrastructure investment and proactive co-operation with foreign partners are among the most important lessons from the UK (European Union 2016).

India

With a growing digital economy, India has serious cybersecurity issues. Despite implementation delays, the 2023 Digital Personal Data Protection Act creates a thorough framework for data protection. India's emphasis on protecting vital assets is exemplified by programmes like the National Critical Information Infrastructure Protection Centre (NCIIPC). Nonetheless, it faces difficulties because of limited capacity and a disjointed regulatory environment.

Botswana

Botswana has made strides in developing a national cybersecurity strategy focusing on building awareness and strengthening institutional capacity (Phahlamohlaka et al. 2022). Given its small size, Botswana deserves praise for its efforts to improve its cybersecurity infrastructure. The Cybercrime and Computer-Related Crimes Act, 2018 offers a legal foundation for dealing with cyberthreats, while the Botswana Communications Regulatory Authority (BOCRA) oversees ICT growth and security. To solve capacity shortages, Botswana is exemplary in using regional collaborations and customising tactics to local settings.

Singapore

With a developed ecosystem backed by the Cyber Security Agency (CSA), Singapore stands out as a global leader in cybersecurity. The country's cybersecurity strategy integrates international co-operation, business sector engagement and public awareness in a comprehensive approach. Singapore's achievements demonstrate the importance of a proactive, all-encompassing approach to cybersecurity. Singapore's emphasis on international co-operation is one of its distinguishing features. It actively contributes to improving cybersecurity internationally through bilateral agreements, partnerships with international organisations and involvement in regional forums such as the Association of Southeast Asian Nations (ASEAN) (Ee 2024).

Fiji

Fiji has introduced regional collaboration efforts to address cybersecurity threats, leveraging partnerships with larger nations and organisations (Tamanikaiwaimaro 2021). Fiji regularly interacts with institutions like the United Nations and regional initiatives like the Pacific Islands Forum to develop strong cybersecurity frameworks.

Eswatini

Eswatini's initiatives include public-private collaborations for ICT infrastructure development. Resource constraints and limited public awareness hinder progress (Nchake and Shuaibu 2022). Through various programmes, such as encouraging public-private partnerships targeted at improving ICT infrastructure, Eswatini has made

significant progress in developing its ICT sector. These partnerships have made it easier to roll out digital tools and increase internet access to boost economic growth and enhance service delivery in industries including agriculture, healthcare and education. Methods to address these issues include initiatives to raise funds to close resource shortages, efforts to advance ICT literacy, and capacity-building programmes to improve digital skills. Eswatini hopes to establish itself as a competitive participant in the global ICT scene and to foster a more inclusive digital economy by concentrating on these areas.

Lessons learned from successes and failures

Invest in leadership and institutions: Nations with specialised institutions, like Singapore's CSA or the UK's NCSC, are better equipped than others to handle cyber threats. Co-ordination and consistent focus among stakeholders are guaranteed by institutional leadership.

Adjust frameworks to local contexts: Although EU models such as the GDPR offer helpful standards, frameworks must be modified to consider regional legal, cultural and economic circumstances.

Fill the capacity gaps: Countries with limited resources frequently find it difficult to implement thorough cybersecurity safeguards. These gaps can be closed through focused collaboration, technology and educational initiatives.

Encourage regional and global co-operation: No nation can handle cyber threats on its own. Cyber threats are international. Successful examples that highlight the value of co-operation include Singapore's involvement in international forums.

Avoid fragmented approaches: Inconsistent policies and a lack of agency collaboration impede cybersecurity efforts. Better outcomes are obtained through integrated approaches as demonstrated in Singapore and the UK.

Raise public awareness: At local level, resilience is improved by educating people about cybersecurity threats and best practice.

Lack of political will, inadequate finance and an excessive dependence on outside solutions without local capacity building are frequent causes of failure. A long-term vision and consistent dedication are needed to address these problems.

8. Policy recommendations

To improve cybersecurity and privacy governance in the Commonwealth, effective policy suggestions must consider the diverse capacities of member countries while striking a balance between short-term demands and long-term objectives. This section presents customised implementation plans for both the short and long term, with a focus on methods that consider the difficulties faced by high-capacity and low-resource nations.

Short-term strategies

Adopting or revising cybersecurity and privacy laws to improve their legal and regulatory frameworks should be a top priority for member countries. As a starting point, low-resource nations should adopt adaptable baseline norms like the African Union Convention on Cyber Security and Data Protection (Malabo Convention). High-capacity nations ought to concentrate on improving current legislation to consider cutting-edge technology like the Internet of Things (IoT) and AI.

Create national cybersecurity plans. Creating a national cybersecurity plan offers a way of dealing with weaknesses. Plans for safeguarding vital infrastructure, capacity-building programmes and risk assessments should all be part of these.

Boost public awareness campaigns. Educating people about privacy and cyber hygiene is an affordable way of improving resilience on a personal level. Governments should work with the business sector and civic society to produce easily available instructional materials.

Establish regional support networks. To exchange resources and experience, Commonwealth countries should set up regional cybersecurity hubs. Smaller countries with fewer resources can particularly benefit from these hubs' ability to function as training, research and incident response facilities. One important short-term step is to increase incident response capacity by establishing CERTs in each member country. CERTs can facilitate information sharing among stakeholders, offer technical support and organise responses to cyber incidents.

Long-term strategies

Create strong institutional frameworks by fortifying national cybersecurity agencies and establishing independent data protection authorities (DPAs). These organisations ought to have the funding and legal standing necessary to compel adherence to regulations and to direct the creation of new ones.

Invest in education and workforce development. Member countries should place a high priority on developing a workforce with the necessary skills by funding professional training programmes and cybersecurity education. Scholarships, internships and certification can be funded, in part, through public-private partnerships.

Encourage regional and global harmonisation: Bringing cybersecurity and data protection standards into line throughout the Commonwealth will ease cross-border collaboration and lessen regulatory fragmentation. The goal of member countries should be to conform to international agreements like the Budapest Convention on Cybercrime.

Leverage emerging technologies. To improve data security and threat detection, governments should investigate the application of blockchain, AI and machine learning. Blockchain, for instance, can guarantee data integrity, while AI can examine significant volumes of data to detect threats early.

Promote sustainable funding models. Countries with limited resources can receive sustainable funding by creating cybersecurity trust funds or applying for international development assistance. High-capacity nations should provide financial and technical assistance for regional projects.

Tailored approaches for low-resource and high-capacity countries

Low-resource countries ought to concentrate on basic projects that require little funding but have a significant impact. These include focusing public awareness efforts, utilising regional hubs for knowledge and implementing baseline legal frameworks. Local resources can be enhanced through collaboration with private sector groups and foreign organisations.
High-capacity countries might set the standard by showcasing the usefulness of cutting-edge frameworks and technologies. Innovation, cross-border co-operation, and offering technical support to member countries with fewer resources should be their top priorities. High-capacity countries can contribute to strengthening the Commonwealth's overall cybersecurity resilience by serving as mentors.

9. Conclusion

This paper has covered important issues, opportunities and tactics for improving cybersecurity and data protection in the Commonwealth. The diversity of Commonwealth countries presents both opportunities and challenges for developing common cybersecurity standards. Diverse institutional and regulatory frameworks make it difficult to share data across borders and to work together to combat cyber threats. Many member countries face major obstacles due to a lack of resources and a lack of skilled workers, especially in low-income areas. Through the Commonwealth Cyber Declaration and the CTO's operations, for example, the Commonwealth has made progress in promoting collaboration despite these obstacles.

The paper also highlights successful national and regional initiatives including the significance of customised strategies that adhere to international standards while respecting local situations.

Reflections on fostering a safer and more secure digital environment

Three fundamental tenets – inclusion, innovation and international co-operation – are essential for a secure digital environment in the Commonwealth. Regardless of ability, inclusivity guarantees that all member countries have the resources and assistance required to safeguard their digital ecosystems. The creation of innovative solutions to counteract ever-changing cyber threats is fuelled by innovation. International co-operation makes it possible to pool resources, share knowledge and take co-ordinated action to address shared problems.

Strong public-private partnerships, ongoing governmental commitment, and the active participation of civil society are all necessary to achieve these objectives. Policymakers need to understand that data protection and cybersecurity are not merely technical problems. Rather, they are essential to social progress, economic growth and national security.

Call to action for policymakers, institutions and international bodies

Policymakers should make cybersecurity and data protection a top priority on national agendas and provide enough money and legislative backing. They should participate in multilateral discussions to align national policies with regional and international norms.

Institutions should enforce the law, control hazards, co-ordinate actions, strengthen institutions and establish new ones as needed. They should invest in research and development to keep ahead of new dangers.

International organisations should increase capacity-building programmes aimed at low-resource nations while guaranteeing fair access to financial support and technical assistance. They should encourage the exchange of case studies and best practice to foster innovation and knowledge transfer.

10. References

African Union (2014), African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), available at: https://au.int

Arora, R and Luthra, S (2021), 'Challenges in cybersecurity policy implementation: A Commonwealth perspective', *Journal of Cyber Policy*, 6(2), 123-145.

Bada, M and Nurse, JRC (2019), 'Cybersecurity education and awareness: A systematic review of research and trends', *Computers & Security, 88*, 101613, available at: https://doi.org/10.1016/j.cose.2019.101613

Clarke, R (2019), 'Understanding the complexities of data protection in the digital age', *Information Security Journal*, 28(3), 190-202.

Commonwealth Secretariat (2018a), 'Enhancing cybersecurity in the Commonwealth: Key strategies and initiatives', *Commonwealth Reports*, 45, 89-104.

Commonwealth Secretariat (2018b), *The Commonwealth Cyber Declaration*, available at: https://thecommonwealth.org

Commonwealth Secretariat (2018c), *Cybersecurity and the Commonwealth: Advancing National and Regional Approaches to Cybersecurity Policy*.

Commonwealth Telecommunications Organisation (2019), *The State of Digital Transformation in Commonwealth Countries*.

Cyber Security Agency of Singapore (CSA) (2021), Singapore Cybersecurity Strategy 2021, available at: https://www.csa.gov.sg

Daly, A (2020), *Privacy, Data Protection, and Cybersecurity in the Commonwealth*. Cambridge University Press.

DataGuidance (2020), *Kenya's Data Protection Act: An Overview*, available at: www.dataguidance.com

Ee, SKE (2024), US-Singapore cooperation on tech and security: Defense, cyber, and biotech, *arXiv preprint arXiv:2408.07946*.

European Union (2016), 'General Data Protection Regulation (GDPR)', *Official Journal of the European Union, L119, 1–88*, available at: https://eur-lex.europa.eu

Greenleaf, G (2021), *Global data privacy laws 2021: 145 national laws and many bills*, Privacy Laws & Business International Report.

Information Commissioner's Office (ICO) (2021), *Guide to the UK General Data Protection Regulation (UK GDPR)*, available at: www.ico.org.uk

International Telecommunication Union (ITU) (2021), *Global Cybersecurity Agenda*. Available at: www.itu.int

International Telecommunication Union (ITU) (2022), *Global Cybersecurity Index*. Available at: www.itu.int

Johnson, D (2017), 'Cybersecurity frameworks in advanced economies: Lessons from Canada and the UK', *Global Cybersecurity Review*, 10(1), 34-50.

Mistry, P (2022), 'Advancing cybersecurity collaboration in the Commonwealth', *Commonwealth Studies Quarterly*, 29(4), 67-81.

Nchake, MA and Shuaibu, M (2022), 'Investment in ICT infrastructure and inclusive growth in Africa', *Scientific African*, 17, 10.1016/j.sciaf.2022.e01293.

Office of the Australian Information Commissioner (OAIC) (2020), *Privacy Act 1988 Overview*, available at: www.oaic.gov.au

Personal Data Protection Commission (PDPC) (2022), *Personal Data Protection in Singapore: Guidelines and Resources*, available at: www.pdpc.gov.sg

Phahlamohlaka, J, Theron, J and Aschmann, MJ (2022), 'National cybersecurity implementation in South Africa: The conundrum question', *Journal of Information Warfare,* 21(1), 1-16.

Radu, R (2021), 'The harmonization of data protection policies across the Commonwealth: A pathway for innovation and governance', *Journal of International Policy, 14*(2), 223-244, available at: https://doi.org/10.1016/j.jip.2021.14.223

Shackelford, S (2012), 'Rethinking cybersecurity: Global perspectives', *American Journal of International Law*, 106(3), 569-607.

Sharma, N (2020), 'Emerging cyber threats and their implications for Commonwealth nations', *Digital Security Quarterly*, 15(3), 45-60.

Smith, J, Taylor, R and Green, H (2020), 'Data breaches and socio-economic impacts', *Cyber Studies Review*, 22(2), 210-229.

Tamanikaiwaimaro, S (2021), *Cybersecurity in the Republic of Fiji*, DiploFoundation, available at: https://www.diplomacy.edu/wp-content/uploads/2021/06/IGCBP2010_2011_Tamanikalwalmaro.pdf

United Kingdom Government (2018), Data Protection Act 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/contents

United Nations Conference on Trade and Development (UNCTAD) (2021), *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. United Nations.

Weber, M (2020), 'Collaborative approaches to data protection in international organizations', *International Journal of Cyber Studies*, 18(1), 75-92.

World Economic Forum (2020), *Cybersecurity and the Digital Economy: Lessons from Leading Nations*, *The Global Risks Report 2020*, available at: https://www.weforum.org

About the authors

Otshepeng Mazibuko PhD (c) is at the University of Pretoria and a researcher assistant on the Public Understanding of Big Data and Genomic Medicine in Africa project at the University of Cape Town. Her interdisciplinary work blends robust theoretical frameworks with practical expertise in research, project management, and policy advocacy, gained through roles such as Research Consultant at the Southern African Trust. Her doctoral research critically examines decentralisation processes in South Africa, aiming to influence governance and reverse systemic inequalities through innovative, impactful solutions.