Chapter 4

Principles and Recommendations

Chapter 4
Principles and Recommendations

The Commonwealth Charter recognises the inalienable right of individuals to participate in democratic processes, in particular through free and fair elections. Governments, political parties and civil society are all responsible for upholding and promoting democratic culture and practice and are accountable to the public in this regard. International human rights law, in particular through the UN International Covenant on Civil and Political Rights (ICCPR), also enshrines the right to take part in the conduct of public affairs, and to vote and to be elected at genuine periodic elections by universal and equal suffrage, held by secret ballot.

In today's world of increasing reliance on information and communication technologies, including in electoral processes, countries and individuals have a shared interest in protecting the security of networks, data, the people that use them and the services that run on them. The Commonwealth Cyber Declaration, adopted by Heads of Government at their meeting in 2018, highlights the importance of a free, open, inclusive and secure cyberspace, achieved through the importance of common standards and the strengthening of data protection and security frameworks. It also highlights the importance of tolerance and respect for diversity and understanding in cyberspace and affirms that the same rights that citizens have offline must also be protected online.

In this section, we highlight four key principles relating to election cybersecurity that emerge from Commonwealth and international instruments, together with the specific recommendations made by this guide in relation to each.

4.1 Democratic self-determination

Individuals have an inalienable right to participate in democratic processes, in particular through free and fair elections. This includes a commitment to peaceful, open dialogue and the free flow of information, including through a free and responsible media, and to enhancing democratic traditions and strengthening democratic processes.[1] All peoples have the right to self-determination and the opportunity to take part in the conduct of public affairs, directly or through freely chosen representatives.[2]

Recommendations

- Governments should develop modernised laws and institutions to protect elections, addressing cybersecurity, cybercrime, data protection and telecoms/media regulation issues.
- EMBs should ensure their cybersecurity guidance is well disseminated via voter education programmes and media training/guidance and should maximise transparency more broadly in their systems and processes.
- EMBs should carry out or **facilitate assessment** of the interaction effects between the use of electoral technology and security provisions and other structural features and challenges of the **democracy, such as literacy, accessibility,** and **ethnic and gender dimensions.**
- Commonwealth countries should consider legislating to ensure that platforms and advertising networks are obliged to make political adverts public, in line with best practices in the area which allow public research and scrutiny.
- Commonwealth countries may be aided by a template agreement with social media companies for national memoranda of understanding relating to disinformation, potentially based on the EU Code of Practice.
- Commonwealth countries should strengthen reporting and publication of political spending online, as well as offline, and should monitor donations and uses of 'dark money' to try to influence campaigns.
- EMBs should ensure the availability of cybersecurity training for political parties, in collaboration with national actors best placed (and seen as legitimate) to deliver such training.
- Where non-resident citizens are enfranchised, provision of online electoral information and forms for printing and returning by post present significantly lower cybersecurity risks than remote voting.

4.2 International law and co-operation

The principles of international law and co-operation, international peace and security, sustainable economic growth and development, and the rule of law are essential to the progress and prosperity of all. An effective multilateral system based on inclusiveness, equity, justice and international law is an important foundation for achieving consensus and progress on major global challenges.[3] Commonwealth countries are committed to the Universal Declaration of Human Rights, and that the same rights that citizens have

offline must also be protected online.[4] International human rights law also provides that no-one shall be subjected to arbitrary or unlawful interference with his or her privacy, and that everyone shall have the right to freedom of expression.[5]

Recommendations

- Governments should co-operate on electoral cybersecurity via the Commonwealth, regional co-operation organisations such as the Caribbean Community (CARICOM), the Association of Southeast Asian Nations (ASEAN), the African Union, the Organization of American States (OAS) and the Organization for Security and Co-operation in Europe (OSCE), and other intergovernmental bodies such as the International Institute for Democracy and Electoral Assistance (International IDEA).
- EMBs should develop mechanisms to enable information sharing across the Commonwealth on threats, vulnerabilities and detected attacks against election infrastructure.
- Commonwealth countries should look for opportunities to work with relevant non-governmental organisations, such as the Forum of Incident Response and Security Teams (FIRST), the International Foundation for Electoral Systems (IFES) and the Commonwealth Telecommunications Organisation (which works extensively with ministers of telecommunications and computer emergency response teams).
- Commonwealth EMBs should provide peer support and review on cybersecurity to their neighbouring EMBs, as well as sharing training opportunities.
- EMBs should co-operate to explore common standards for election cybersecurity products and services, to stimulate the development of efficient markets of providers. These standards should include secure configuration by default, along with consideration of the liability of vendors
- EMBs – and funders of election digitisation programmes – should aim for maximum transparency of contracts with suppliers, and of funding arrangements.
- Commonwealth EMBs should work with election observation organisations to develop comprehensive schedules of cybersecurity indicators, covering the entire electoral lifecycle, to be observed during missions.

- Electoral observation teams should include the technical expertise needed to effectively monitor digitised electoral processes.
- Exemptions or lower restrictions for data processing in data protection and privacy laws for political organisations or purposes must be narrow and proportionate.
- Governments should ensure privacy and data protection laws are in place to protect voter data wherever it is held, including in the private sector. These laws should allow political parties and candidates to engage with voters; but any exemptions that affect voters' trust or data protection and security should be carefully limited.
- The data protection and/or privacy regulator with competence for political and electoral issues must be independent from government and adequately resourced and empowered.
- States without a data protection or privacy law should look to enact one in line with existing international standards and institutional practices.
- EMBs should not request the operation of internet shutdowns during election periods, or at any other point not objectively assessed as a national emergency and sanctioned by a superior court.
- Commonwealth countries should in general keep the internet on amid disinformation and cybersecurity concerns, while ensuring that false announcements are removed and countered where fraudulent or casting doubt on official EMB results and guidance (which are generally against the terms of service of major social media platforms
- Disinformation is best tackled by governments through media pluralism and literacy initiatives, as these allow diversity of expression and choice. For social media platforms, source transparency indicators and deprioritisation of information rated false by independent fact checkers will limit impact. Users need to be given the opportunity to understand how their search results or social media feeds are built, and to edit their search results/feeds where desirable.
- Freedom of expression as a fundamental right should be subject only to appeal rights equivalent to those under state regulation, and thus disinformation should be regulated by legislation with appeal to courts of law. Options to ensure independent appeal and audit of platforms' regulation of their users should be introduced. When technical intermediaries need to moderate content and accounts, detailed and transparent policies, notice and appeal procedures, as well as regular reports, are crucial.

4.3 Strengthening the use of ICTs for elections while enhancing their security

Information and communication technologies are powerful instruments of development: delivering savings, efficiencies and growth in economies, as well as promoting education, learning and the sharing of culture.[6] Strengthening the use of such technologies, while also enhancing their security, can lead to more efficient and accurate election processes, while recognising the threats to stability in cyberspace and the integrity of critical infrastructure. There is a shared interest in protecting the security of networks, security of data, the people that use them and the services that run on them.[7]

Recommendations

- EMBs should give careful consideration to use of technology in the elections process if and where it demonstrably addresses a clear need, while carefully managing the resulting cybersecurity risks with measures that are proportionate.
- Cross-government (including EMBs, national cybersecurity centres, state and local government agencies, data protection and media/telecoms regulators) co-ordination, and co-operation with political parties, traditional and new media, and civil society are key to effective action and societal trust in elections. A standing multistakeholder election security group should manage preparation and directly oversee the election process, trigger continuity plans, and communicate with the media and parliamentary oversight bodies.
- EMBs and national cybersecurity agencies should consider whether designation of key election systems as part of critical national infrastructure will improve their security.
- EMBs must model and mitigate the potential of insider attacks, both within their own activities and those of other electorally relevant organisations, such as political parties. Existing anti-corruption efforts, non-disclosure agreements and strong access controls are useful tools in this context.
- Individuals with reading – and especially writing and administrative – access to significant systems should be security vetted to an appropriate level. While government security agencies may carry out vetting, for independence reasons, EMBs should retain the ultimate decision as to staff appointments.
- EMBs should regularly audit automated systems used for electoral planning for integrity, and put in place processes to ensure documentation and assurance of the provenance of data sources being used.

- EMBs should be aware of and seek to mitigate cybersecurity risks involving contractors for electoral logistics, especially those with systems directly linked to the EMB.
- Cybersecurity threat assessment and mitigation should be undertaken regularly by EMBs as part of an ongoing process, rather than in the run-up to ballot periods alone.
- Information about polling locations should be delivered from EMBs to voters in a secure and robust manner, with monitoring of the veracity and timeliness of information provided.
- An independent agency, such as a data protection authority (DPA), should have competences over the privacy and security of electoral data, including its processing, storage and transformation into derivative data by political parties.
- EMBs should take steps to ensure that only electoral roll data necessary for the intended purposes of use are transmitted to authorised actors, in a format which does not encourage inappropriate reuse or dissemination and including fingerprinting data to facilitate the tracing of data breaches.
- EMBs and their cybersecurity partners should identify all avenues, actors and systems which feed into and are informed by the electoral roll(s), and should map out security threats and capacities, contact points and regular procedures to check for data and system integrity.
- The master copy of the electoral roll(s) should not be connected to public networks and should only be updated with additional information in accordance with procedures designed to ensure the integrity and provenance of the new information.
- When engaging in data cleaning or validation, the responsible agency should keep complete tamperproof logs of all changes made and use technologies which allow such logging. This allows for detection of integrity issues and specific rollbacks if such issues are discovered.
- EMBs and their cybersecurity partners should ensure providers, domain and hosting services for any online registration are easily contactable, identify periods where availability is critical (e.g. near electoral deadlines) and should designate a specific team or individual as responsible to respond to system issues.
- EMBs should prepare and practise backup procedures where availability attacks on critical systems might disrupt electoral processes.

- Where machines are used to cast votes, EMBs should carefully consider the use of voter verified paper audit trails to enable every vote to be verified where results are disputed.
- Systems to verify postal ballots should be carefully designed to maintain public trust and the confidentiality of votes.
- EMB officials should examine and determine how to treat every ballot rejected by automatic counting systems as invalid or uncertain.
- EMBs should have in place procedures for ongoing secure configuration and testing of all systems used in elections, with regular exercises to test responses to attacks.
- EMBs should consider obtaining external certification of security-critical elements of election infrastructure to build public trust.
- Before introducing internet voting systems in elections, EMBs should assess very carefully the cybersecurity risks they introduce, as well as the extensive mechanisms required to manage that risk and potential damage to voter trust in case of disputed outcomes.
- EMBs should ensure results transmission systems (RTSs) are secure, subject to clear and strict access controls, and have appropriate levels of redundancy and backup procedures in place should components of them unexpectedly fail.
- EMBs can improve the resilience of results reporting, as well as public confidence in the results, by supporting parallel vote reporting and tabulations by civil society organisations.
- EMBs should ensure software used in vote tabulation is audited and verified, and used by trained staff on appropriately secured hardware.
- EMB websites, especially those announcing election results, should be protected against high levels of traffic and denial of service attacks.
- EMBs should develop regularly updated processes for auditing the use of election technologies, and consider how far these processes and their results can be made accessible to observers and the public.
- EMBs and/or their cybersecurity partners should actively monitor election infrastructure for intrusions, as well as having the capability to rapidly escalate and respond during election periods at the direction of senior decision-makers.
- EMBs should provide cybersecurity training for all staff, as well as career development for technical staff, partnering with local universities, regional peers and international organisations.

4.4 Non-discrimination

The International Covenant on Civil and Political Rights (ICCPR) provides that all persons are equal before the law and are entitled without any discrimination to the equal protection of the law. This includes without distinction of any kind such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

The Commonwealth Cyber Declaration recognises that access to information and digital literacy can be a powerful catalyst for economic empowerment and inclusion. Through the declaration, Commonwealth countries have committed to take steps towards expanding digital access and digital

Figure 4.1 Pakistan's legal requirement for special measures to register women voters

inclusion for all communities without discrimination and regardless of gender, race, ethnicity, age, geographic location or language.[8]

Recommendations

- EMBs should ensure their cybersecurity guidance is well disseminated via voter education programmes and media training/guidance and should maximise transparency more broadly in their systems and processes.
- EMBs should carry out or facilitate assessment of the interaction effects between the use of electoral technology and security provisions and other structural features and challenges of the democracy, such as literacy, accessibility, and ethnic and gender dimensions.
- EMBs using biometric authentication should ensure all eligible voters are easily able to register and vote.
- Given the potential cybersecurity implications of requiring biometric or other electronic identification systems, EMBs should gather a clear evidence base on the impact on fraud, turnout and system impact, particularly among marginalised communities.
- EMBs should enable the use of technologies that improve the accessibility of elections for disabled people, while evaluating and carefully managing any resulting cybersecurity risks.

4.5 Conclusion

Commonwealth countries use digital election technologies in a variety of ways – to more efficiently administer electoral registers and communicate results; to authenticate voters using biometric technologies; and to enable voters to register more easily and check details of polling venues. **Electoral authorities should continue to give careful consideration to use of technology in the elections process if and where it demonstrably addresses a clear need, while carefully managing the resulting cybersecurity risks, with measures that are proportionate to the risk.**

> *We must not … make the mistake of placing our faith in technical solutions to political problems. When opposition parties and donors invest in the transformative power of new scientific advances, they often overlook the fact that even the most advanced forms of election technology rely on human programming and management. And there is nothing about digital technology that means that those who use it are likely to be any more trustworthy or fair. As John Githongo, Kenya's former anti-corruption tsar, has put it: 'You cannot digitise integrity'.*[9]

At the same time, EMBs must ensure that financial, human and other resources applied to new digital technologies do not come at the expense of defending against the many types of election interference that have little to do with technology, including 'intimidation, vote buying, media bias, low participation by women, the abuse of state resources by incumbent parties or endemic political and electoral violence'.[10] Donors supporting elections in two African Commonwealth countries, reported in 2018 that support for 'purchasing expensive equipment inevitably means they are forced to invest fewer resources in domestic observation unless there are exceptional reasons to increase the overall budget'[11] – and if technologies fail and backup manual processes must be used instead during polling, 'opposition parties and donors often find that their focus on new technology has actually undermined their capacity to detect fraud'.[12]

During each phase of elections, the direct and indirect use of computers and other technology introduces a range of risks to electoral integrity. These pose threats to confidentiality, integrity, and availability of information and infrastructures concerning votes and voters, candidates and parties, and broader election processes. In this guide, we have analysed these risks at each phase of the election cycle and made a series of recommendations on best practices to manage them appropriately, in order to maintain public confidence in elections.

Some of these best practices are deeply technical, involving system testing, certification, monitoring and auditing. EMBs need to plan carefully to meet their future need for technically expert staff, whose skills are in high demand in the private sector.

However, for senior EMB policy-makers, the most important best practices relate to cybersecurity governance and international collaboration. EMBs across the Commonwealth are facing a number of common challenges and can maximise the impact of their cybersecurity measures through shared learning and resources.

These best practices should continue to evolve as technology and its use in elections continues to develop. By working together to address ongoing cybersecurity challenges, Commonwealth electoral authorities can ensure they maintain the public trust in well-run elections that is essential to democracy.

Notes and references

1 The Commonwealth (2013), Commonwealth Charter, signed by Her Majesty Queen Elizabeth II, Head of the Commonwealth, Commonwealth Day 2013, available at: http://thecommonwealth.org/sites/default/files/page/documents/CharteroftheCommonwealth.pdf

2 International Covenant on Civil and Political Rights (1966), adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

3 The Commonwealth (2013), **Commonwealth** Charter.

4 The Commonwealth (2018), Commonwealth Cyber Declaration, clause 5, agreed and signed on 20 April at the 2018 Commonwealth Heads of Government Meeting in London, UK, available at: https://thecommonwealth.org/commonwealth-cyber-declaration
5 International Covenant on Civil and Political Rights (1966).
6 The Commonwealth (2013), Commonwealth Charter, Charter IX.
7 The Commonwealth (2018), Commonwealth Cyber Declaration.
8 Ibid.
9 Nic Cheeseman and Brian Klaas (2019), *How to Rig an Election*, Yale University Press, New Haven, pp.236–237.
10 Democracy Reporting International (2011), 'Electronic Voting Machines: The Promise and Perils of New Technology', briefing paper no. 11, p.3, available at: http://democracy-reporting.org/wp-content/uploads/2016/02/dri_briefing_paper_11_-_electronic_voting_machines.pdf
11 Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization,* 25(8), p.1410.
12 Ibid, p.1410.