Cybersecurity for Elections

A Commonwealth Guide on Best Practice

Advance copy – the information contained is subject to edits.

Contents

Contents ---- 2
Acknowledgments ---- 4
About the authors ---- 5
Figures ---- 6
Boxes ---- 7
Acronyms and glossary ---- 9
Principles and recommendations ---- 11
1. Democratic self-determination ---- 11
2. International law and co-operation ---- 12
3. Strengthening the use of ICTs for elections while enhancing their security ---- 13
4. Non-discrimination ---- 15
Notes and references ---- 16
Chapter 1 Introduction ---- 17
1.1 The increasing vulnerability of electoral systems ---- 17
1.2 The electoral cycle ---- 19
1.3 The Commonwealth context ---- 20
1.4 Relevant organisations and regulatory frameworks ---- 21
Beyond electoral management bodies ---- 21
Relevant regulatory frameworks ---- 23
Other relevant organisations ---- 27
Notes and references ---- 29
Chapter 2 Cybersecurity across the electoral cycle ---- 33
2.1 Election activities across the electoral cycle ---- 34
2.2 Overarching features of direct threats ---- 36
Insider threats ---- 37
Maintaining trust ---- 38
2.3 Planning and logistics ---- 39
2.4 Electoral rolls ---- 40
2.5 Campaigning ---- 46
Attacks on parties and candidates ---- 47
2.6 Voting ---- 48
Voter verification ---- 48
Vote casting ---- 53
Remote voting ---- 57
Vote counting ---- 62
2.7 Communication of results ---- 63
Transmission ---- 63
Tabulation and aggregation ---- 64

Publication---65
2.8 Auditing and challenging results---67
Notes and references ---68
Chapter 3 Overarching best practices for secure elections ---73
3.1 Holistic action---74
3.2 International co-operation ---76
3.3 Cybersecurity risk management ---79
National cybersecurity centres and strategies---79
Public sector capacity and training---82
Ongoing threat assessment ---87
Procurement processes---88
Certification and quality assurance ---89
Building and running secure systems---91
3.4 Privacy and data protection---93
Political exemptions---94
3.5 Electoral campaigns, interference and disinformation ---96
Internet 'switch-off' and disinformation laws---99
Regulating the use of social media to target voters --- 102
Regulatory responses and transparency requirements--- 104
Notes and references --- 106
Chapter 4 Concluding remarks --- 111
Notes and references --- 112

Acknowledgments

The Commonwealth Secretariat acknowledges with gratitude the work of Ian Brown, Chris Marsden, James Lee and Michael Veale in developing the guide, as well as the financial support of the United Kingdom Foreign and Commonwealth Office.

The Secretariat also extends its thanks to the Electoral Commission of Ghana, the Election Commission of Pakistan, the Elections and Boundaries Commission of Trinidad and Tobago and the UK Electoral Commission for hosting research visits, and to all the Commonwealth election management bodies who responded to the questionnaire and provided feedback on the drafts.

The authors additionally wish to thank Ross Anderson, Andy Baines, Sonali Campion, Nic Cheeseman, Alex Folkes, Carina Kabajunga and Steven Malby for their detailed feedback on drafts of this guide. Any errors and omissions remain their own responsibility, and can be notified to electoral.network@commonwealth.int for future updates.

About the authors

Ian Brown is visiting CyberBRICS Professor at Fundação Getulio Vargas in Rio de Janeiro, and an ACM Distinguished Scientist. He was previously Senior Fellow at Research ICT Africa; Principal Scientific Officer at the UK government's Department for Digital, Culture, Media and Sport (DCMS); Professor of Information Security and Privacy at the University of Oxford; and a Knowledge Exchange Fellow with the Commonwealth Secretariat and UK National Crime Agency. His books include *Regulating Code: Good Governance and Better Regulation in the Information Age* (with Christopher T Marsden) and *Research Handbook on Governance of the Internet*. His 2001 PhD in computer and communications security is from University College London (UCL).

Christopher T Marsden has been Professor of Internet Law at the University of Sussex since 2013, and Founder-Director of the Centre for Information Governance Research @SussCIGR. He was formerly Professor of Law at Essex University, having previously taught and researched at Warwick University, the University of Oxford and the London School of Economics (LSE). He is author of five monographs on Internet law: *Network Neutrality: From Policy to Law to Regulation*; *Regulating Code*; *Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*; *Net neutrality: Towards a Co-Regulatory Solution;* and *Codifying Cyberspace*.

James Lee is a Senior Policy Adviser at the Department for Digital, Culture, Media and Sport (DCMS), where he has been leading work on online content policy, and to ensure regulators are equipped for a digital age. He draws on five years of experience in technology policy, notably working for the UK's national technology trade association to represent its members' interests in cyber and national security; here he authored an exploratory report, *Playing Catch Up: Incorporating Distributed Ledgers into the Technology Stack and Repurposing the Wider Ecosystem.* He holds a degree in International Relations from the University of St Andrews.

Michael Veale joined UCL's Faculty of Laws as Lecturer in Digital Rights and Regulation in 2019. He holds a PhD in the application of law and policy to the social challenges of machine learning. He previously worked at the European Commission and holds degrees from Maastricht University and the LSE. Since 2019, Dr Veale has also been Digital Charter Fellow between the Alan Turing Institute, the UK's National Centre for AI and Data Science, and DCMS. He has authored and co-authored reports for a range of organisations, including the Law Society of England and Wales on algorithms in the justice system, the Royal Society and British Academy on the future of data governance, and the United Nations on artificial intelligence (AI) and public services.

Figures

Figure Pakistan's legal requirement for special measures to register women voters 16

Figure 1.1 Threat activity targeting democratic processes observed by Canadian Communications Security Establishment 17

Figure 1.2 Grouping of survey respondent countries

Figure 1.3 International IDEA's levels of multiagency collaboration 23

Figure 1.4 Ghana's National Communications Authority advertises its anti-spam SMS service 24

Figure 1.5 Proportion of respondent Commonwealth countries modernising electoral legislation for cybersecurity threats 26

Figure 2.1 Cyber threats to global democratic processes, observed by Canadian Communications Security Establishment 33

Figure 2.2 The electoral cycle as presented by International IDEA 34

Figure 2.3 Centralised vs decentralised voter registers in respondent Commonwealth countries 42

Figure 2.4 South Africa's voting, counting and results announcement process 48

Figure 2.5 Indelible ink mark made on a South African voter's thumbnail during the 2009 election 49

Figure 2.6 Use of biometric identification by respondent EMBs 52

Figure 2.7 USA vote casting and counting systems by county in 2016 54

Figure 2.8 Types of voting employed across respondent Commonwealth countries 56

Figure 2.9 Proportion of respondent Commonwealth countries where non-residents can vote 58

Figure 2.10 Respondent EMB use of social media 66

Figure 3.1 Proportion of respondent Commonwealth EMBs which have a partnership with the national cybersecurity centre or CSIRT 81

Figure 3.2 Proportion of respondent Commonwealth EMBs which have internal cybersecurity teams 84

Figure 3.3 Proportion of respondent Commonwealth EMBs who have commissioner or board-level cybersecurity representation 86

Figure 3.4 Phases of the IFES HEAT Process (Holistic Exposure and Adaptation Testing).....88

Figure 3.5 Proportion of EMBs which have used international standards (such as those developed by ISO, IEE, the UN, OAS, etc.) in the development of policies, regulations or processes for elections cybersecurity. 90

Figure 3.6 UK Member of Parliament warns of electoral disinformation spreading via WhatsApp during the 2019 general election 97

Figure 3.7 Reported cases of electoral misinformation on social media platforms in respondent Commonwealth countries 98

Figure 3.8 Twitter warns against use of its services to manipulate or interfere in elections99

Boxes

Box 1.1 Models of interagency collaboration....23
Box 1.2 International co-operation by Ghana....24
Box 1.3 Ghana's National Cyber Security Centre....27
Box 1.4 Trinidad and Tobago's Computer Security Incident Response Team (TTCSIRT)....28
Box 1.5 Commonwealth countries with reported (or *proposed, limited or largely uncommenced)* data protection or privacy laws....29
Box 2.1 Aspects of the electoral cycle vulnerable to cybersecurity risks....35
Box 2.2 Targeted confidentiality attacks on political parties and campaigns....36
Box 2.3 Canadian 2011 robocalling scandal....38
Box 2.4 SMS look-up of polling station location in Pakistan....40
Box 2.5 Electoral roll integrity in Pakistan....44
Box 2.6 Voter registration and availability attacks in the UK....45
Box 2.7 Microtargeting and Cambridge Analytica....47
Box 2.8 Biometric voter verification trials in Pakistan....51
Box 2.9 Stolen biometric voter registration kit in Malawi....53
Box 2.10 The interaction of electronic voting machines and fraud in India....54
Box 2.11 India's electronically transmitted postal ballot system....59
Box 2.12 Internet voting trials in Pakistan....62
Box 2.13 Vote counting and collation in Ghana....64
Box 2.14 Results transmission in Pakistan....65
Box 2.15 Results reporting in India....67
Box 2.16 Independent audits of South African elections....68
Box 3.1 Risk management tools and approaches....74
Box 3.2 Cross-government decision-making in Trinidad and Tobago and Ghana....75
Box 3.3 New Zealand cross-agency working....75
Box 3.4 Ghana's media environment....76
Box 3.5 OAS preliminary audit of the Bolivian presidential elections on 20 October 2019....78
Box 3.6 US Department of Justice press release on 2020 election security, 5 Nov 2019....82
Box 3.7 Ghana cybersecurity training initiatives....83
Box 3.8 The UK Cyber *Essentials* scheme....87
Box 3.9 Commonwealth EMB use of cloud computing....89
Box 3.10 ISO/IEC 27000 and other security certifications....91
Box 3.11 NIS election exercise objectives....92
Box 3.12 South Africa's strategic security focus....92
Box 3.13 Structure and provisions of data protection law....93
Box 3.14 Ghana's approach to voter education....97

Box 3.15 Social media tracking centre during 2016 Ghana elections 99
Box 3.16 Singapore's Protection from Online Falsehoods and Manipulation Act 2019 101
Box 3.17 Social media codes of conduct and reporting in Commonwealth countries 103
Box 3.18 Excerpt from the Joint Declaration on Freedom of Expression and 'Fake News'. 104
Box 3.19 The EU Code of Practice on Disinformation..... 105
Box 3.20 Mozilla Foundation recommendations on political advertising archives 105
Box 3.21 NATO Strategic Communications Centre of Excellence Recommendations..... 106

Acronyms and glossary

AI	artificial intelligence
API	application programming interface – allows one piece of software to send and receive data to another and request it to take actions
CERT	computer emergency response team
CNI	critical national infrastructure
CRA	communications (including broadcasting) regulatory authority/agency
CSIRT	computer security incident response team
DDoS	distributed denial of service – a type of online attack where a site and its ISP are flooded with traffic from other devices across the internet, slowing down or stopping the site from responding to legitimate users
DPA	data protection authority (or commission), referred to in some countries as an information or privacy commissioner, responsible for enforcing data protection and privacy laws
DRE	direct recording electronic (machine) – a type of voting machine that records a voter's choice in a polling station
EMB	electoral management body
EVM	electronic voting machine
FIRST	Forum of Incident Response and Security Teams, a global non-governmental association of computer emergency response teams
GDPR	The European Union's 2016 General Data Protection Regulation
GIS	geographic information system – computer tool used to manage and visualise geographical data, such as constituency boundaries
ICCPR	International Covenant on Civil and Political Rights, a core UN human rights treaty
IDEA	International Institute for Democracy and Electoral Assistance, an intergovernmental organisation with 33 members
IFES	International Foundation for Electoral Systems
ISO	International Organization for Standardization
ISP	internet service provider
ITU	International Telecommunication Union, United Nations treaty body for communications

NADRA	National Database and Registration Authority (Pakistan)
NATO	North Atlantic Treaty Organisation, defensive alliance with several Commonwealth countries as members
NCSC	national cyber security centre (or authority) – increasingly common national governmental institutions, for example UK's National Cyber Security Centre
NIS	network and information security
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development – an intergovernmental economics 'think tank' with 36 members
OSCE	Organization for Security and Co-operation in Europe
RTS	Results Transmission System – used to digitally transmit provisional election results from polling and counting centres to Electoral Management Body headquarters
SIDS	small island developing states
SMS	short message service – short text messages sent between mobile phones; used, for example, in Pakistan to provide voters with details of their polling station, and in some multifactor authentication systems
VVPAT	voter verifiable paper audit trail

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.

This guide explains how cybersecurity issues can compromise core aspects of elections, such as maintaining voter lists, verifying voters, counting and casting votes, and announcing results. It also describes how cybersecurity interacts with the broader electoral environment and new ways elections are being carried out, such as campaigns and data management by candidates and parties, online campaigns, social media, false or divisive information, and e-voting. Unless carefully managed, all these cybersecurity issues can present a critical threat to public confidence in election outcomes – which are a cornerstone of democracy.

To help electoral management bodies (EMBs) manage cybersecurity risks, this guide describes **principles for electoral cybersecurity,** as well as **specific organisational recommendations** that can be adapted as required. It additionally signposts an array of more technically detailed materials that can help with specific technical, social or regulatory challenges.

In this overview 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.

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.

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.

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. 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 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.

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

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.

Chapter 1 Introduction

1.1 The increasing vulnerability of electoral systems

Since the 1990s, internet-connected computers, mobile and 'smart' devices have become integral parts of day-to-day life for many in the Commonwealth, including for election-related activities.

During each phase of contemporary 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. *Canada's* Communications Security Establishment has reported that from 2015 to 2018, it observed more than twice as many digital attacks on democratic processes worldwide, and a three-fold increase in Organisation for Economic Co-operation and Development (OECD) countries (see Figure 1.1).[1] These attacks have come from sophisticated state intelligence agencies, as well as 'hackers for hire'[2] and crime gangs targeting organisations for ransoms (as suffered by one Caribbean EMB, which had to pay a bitcoin ransom to regain access to its data).

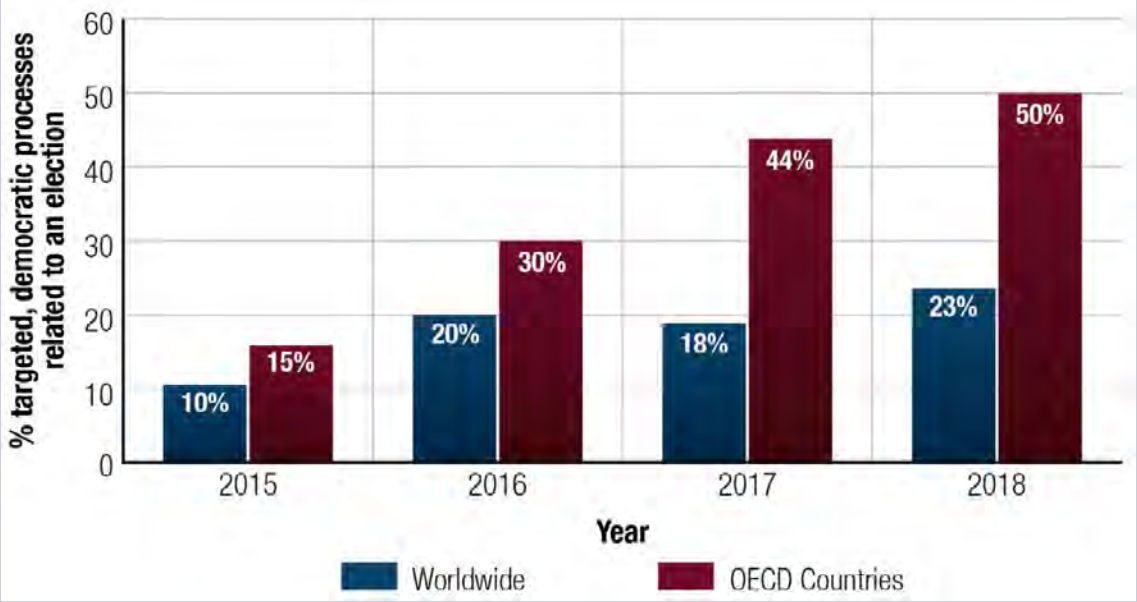


Figure 1.1 Threat activity targeting democratic processes observed by Canada's Communications Security Establishment

This guide explains how cybersecurity issues can compromise traditional aspects of elections, such as maintaining voter lists, verifying voters, counting and casting votes and announcing results. It also describes how cybersecurity interacts with the broader electoral environment and new ways elections are being carried out, such as campaigns and data management by candidates and parties, online campaigns, social media, false or divisive information, and e-voting. Unless carefully managed, all these cybersecurity issues can present a critical threat to public confidence in election outcomes – which are the cornerstone of democracy.

Using digital technology during polling and counting also means that reliable electricity supplies are needed at polling stations and counting centres (with expensive backup facilities), and in some cases (such as checking voter records against remote databases, updating shared lists of individuals that have voted, and reporting preliminary counts remotely), functioning telecommunications links are needed as well. These can by no means be taken for granted in any Commonwealth country – and are another target for both sophisticated and basic attacks.

To help electoral management bodies (EMBs) manage these risks, this guide describes **principles for electoral cybersecurity,** as well as **specific organisational recommendations**

that can be adapted as required. It additionally signposts an array of more technically detailed materials that can help with specific technical, social or regulatory challenges.

***

Cybersecurity covers the broad range of technical, organisational and governance issues that must be considered to protect an information system against accidental and deliberate threats. It goes well beyond the details of firewalls, anti-virus software and similar technical security tools. This breadth is captured in the widely used International Telecommunication Union (ITU) definition:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[3]

The importance of cybersecurity has increased as so many government, business and day-to-day activities around the world have moved online – including election management. But especially in emerging economies, '[m]any organizations digitizing their activities lack organizational, technological and human resources, and other fundamental ingredients needed to secure their system, which is the key for the long-term success'.[4] Although '[o]ne of the claims made for digital technology is that it can strengthen electoral processes in countries where state and electoral management bodies have limited capacities', 'ensuring that such technology is properly used is far from straightforward … additional timelines and training requirements, not greater simplicity, are often the corollaries of digitization'.[5]

Cybersecurity of elections includes issues concerning electronic voting infrastructure, but is not limited to that alone. For example:

- In the *US* state of Georgia, a security researcher found a vulnerability that allowed him to download and potentially alter the register of 6.7 million voters on an insecure election server, as well as instructions and passwords for election workers to log in to systems used to verify voters on election day.[6]
- During the 2016 elections in *France*, the *USA* and *Germany*, hackers released information such as internal e-mails stolen from political parties and candidates in an attempt to damage their credibility – with serious allegations of the involvement of other countries.[7]
- Foreign organisations have been accused of planting and facilitating the spread of misleading and inaccurate information on social media in the run-up to recent elections.
- Journalists and electoral observers are core parts of oversight in electoral systems, but are also personally and organisationally vulnerable to cybersecurity threats.

This guide gives decision-makers in Commonwealth EMBs and related government organisations the information they need to understand and manage these risks. It considers a range of threats throughout the electoral cycle, promoting a systemic view of these fast-moving issues. It also recommends best practices in election cybersecurity, gathered using a literature review; a detailed survey of Commonwealth governments (with responses from 47 per cent of members); an in-depth document review and stakeholder interviews in four Commonwealth countries (*Ghana*, *Pakistan*, *Trinidad and Tobago*, and the *United Kingdom*); workshops in Oxford (with Caribbean parliamentarians), London (with EMB officials from across the Commonwealth), Johannesburg (with African Commonwealth EMB officials), Sydney (with Asian, Pacific and Australasian Commonwealth EMB officials) and Port of Spain (with Caribbean Commonwealth EMB and cybersecurity officials); and interviews with private sector and civil society experts.

To better illustrate the survey responses for comparative purposes, we have grouped respondent countries as follows: using the UN Conference on Trade and Development list of small island developing states (SIDS),[8] the remaining countries in the World Bank's lists of low- and middle-income countries, and high-income countries. SIDS face particular challenges

in terms of electoral infrastructure, but are able to take measures (such as face-to-face verification of voter registrations) that would be too resource intensive for larger countries.

Small island developing states	Other low- and middle-income countries	High-income countries
Barbados	Bangladesh	Australia
Dominica	Botswana	Canada
Fiji	Cameroon	Malta
Grenada	Ghana	New Zealand
Jamaica	India	Singapore
Mauritius	Malaysia	UK
Samoa	Pakistan	
Solomon Islands	Sri Lanka	
Saint Kitts and Nevis		
Saint Lucia		
Trinidad and Tobago		

Figure 1.2 Grouping of survey respondent

1.2 The electoral cycle

Elections are not a singular event, but rather a process which is cyclical in nature and with key defined phases, namely the pre-election period, election period and the post-election period.

- ***In the pre-election period***, EMBs, alongside the national and local government agencies they share responsibilities with, manage the geographical boundaries of constituencies; maintain accurate and complete electoral registers; ensure and maintain the readiness of the electoral system in the context of fast-moving political developments; and often promote democratic engagement, such as encouraging voter registration, training and education. Party registration and party funding and membership are often managed using online systems, and the security and validity of each may need auditing, notably where cybersecurity may be compromised by anonymous online funding, pseudonymous and unverified membership, and impermissible corporate and overseas donations. Misuse of electoral registers of voters and party members can occur due to cybersecurity incidents and misuse of voter registration data. Secure and trustworthy supply chains for voting supplies, such as secure paper and printing, should be in place and be reliable for electoral events. Specialist technical systems used during the elections, such as voter biometric authentication and ballot-counting equipment, must be updated and tested.
- ***Throughout election periods***, EMBs monitor political party and campaign spending against permissible limits, and against foreign interference. Broadcasters are often subject to specific electoral campaign regulation by communications regulatory authorities (CRAs), working in conjunction with EMBs to ensure advertising is legally constituted and funded, and that editorial is not biased in favour of any one party (notably the governing party, or that which is favourable to the broadcaster-owner interest). Other forms of mass media may also be subject to the CRA or EMB's regulations, including newly drafted rules for online and social media advertising and against disinformation.
- ***As elections near*****,** EMBs plan the location and staffing of polling and counting stations, with ballot periods varying across the Commonwealth – from one day in many countries to six weeks in the 2019 *Indian* general election. EMBs must ensure there will be sufficient local polling stations, and that these will be staffed and equipped, and remain open until the appointed closing time, with those waiting in line able to be processed safely and securely. EMBs must ensure access to democratic processes for voters resident in other countries, voters with disabilities, and voters from marginalised populations and minority

(including indigenous) language groups. Where applicable, postal votes, proxy votes or votes in overseas locations must be certified, safeguarded and kept secure until official counting begins.

- ***On election day***, polling officials must be able to check voters are eligible and record they have cast their vote, whether this is with printed lists, online systems and/or biometrics such as using the fingerprints of voters.[9] Most Commonwealth countries still use paper ballots marked by voters, but some such as *India* (which has a multi-week voting period) have introduced voting machines at polling stations. Others, such as the *UK*[10] and *Pakistan*,[11] have conducted subnational trials with remote electronic voting. EMBs must also have communication and response systems to respond to any detected incidents or allegations of electoral impropriety.
- ***Once voting is complete***, ballots are counted. In some countries, this occurs at polling stations; in others, at regional centres. Counting is done by hand in many instances. Several countries use optical scanning machines with human checks, while in some currently limited cases counting is done by tallying digitally reported votes. The count is often a fast-moving race against the media and candidates themselves, and contention or controversy at this stage can threaten the democratic process. EMBs often also play a role beyond tallying and certification in final reporting. The misreporting of results by political parties and others may need to be acted on by the police working in conjunction with the EMB, with some Commonwealth countries imposing social media blackouts during the counting period – and more controversially, during the election day or even campaign.
- ***Finally, in the post-election period,*** EMBs scrutinise results and reflect on the election. This usually requires collecting data and reflecting on successes and failures in the electoral process, but it may also involve responding to requests from courts for access to detailed evidence to decide any challenges to results. EMBs may also report to government and parliament, in some cases requesting reform of the legal powers which enable their functions, notably where cybersecurity and other threats have emerged in the electoral cycle.

1.3 The Commonwealth context

Through the Commonwealth Charter, the member countries of the Commonwealth are all committed to democracy, the rule of law, good governance, separation of powers and human rights.[12] Most have common law legal systems and many have developed comparable institutional environments.

Many members have very similar approaches to cybercrime and data protection law and institutions, shaped by international consensus around Commonwealth model laws and the Council of Europe's cybercrime[13] and data protection[14] conventions, alongside technical assistance from both bodies. Cross-government cybersecurity programmes/centres and independent data protection authorities support these developing regulatory areas. Many member countries have similar approaches to media and telecommunications regulation, often influenced by the British Broadcasting Corporation as a public sector broadcaster, and the *UK*'s integrated Office of Communications regulatory model, covering telecommunications, radio spectrum, broadcasting and post.[15]

Commonwealth members vary significantly in size, population and gross domestic product (GDP) per capita. There are 31 small countries, mainly in the Caribbean Sea and Indian and Pacific Oceans. Many of these developing countries' governments have limited resources, and may not have a permanent EMB or substantial election infrastructure. There are large emerging economies such as *Ghana*, *Kenya*, *Malaysia*, *South Africa*, *Sri Lanka*, *Tanzania* and *Uganda*, with varying levels of digital election infrastructure. There are also some of the world's largest democracies (*Bangladesh*, *Nigeria*, *Pakistan* and *India*), with some sophisticated electoral infrastructure and piloting and use of biometrics and voting machines. And finally, there are advanced economies with sophisticated cybersecurity resources – *Australia*, *Canada*, *New Zealand*, *Singapore* and the *UK*.

The Commonwealth Cyber Declaration, adopted by Heads of Government at their London meeting in March 2018, brought together a long history of Commonwealth work and principles on cyber-related issues. More than 15 years ago, Commonwealth law ministers, for example,

adopted model legislation on computer and computer-related crime, on the protection of personal information, on privacy, on electronic evidence and on electronic transactions. The Commonwealth Cybercrime Initiative, consisting of 35 organisations, including Interpol, OAS, the Council of Europe, the Commonwealth Telecommunications Organisation (CTO) and the ITU, delivered needs assessment services, as well as technical assistance and capacity building, using such tools.

Building on this foundation, Commonwealth countries expressed a shared commitment in the Commonwealth Cyber Declaration to a cyberspace that supports economic and social development and rights online, to build the foundations of an effective national cybersecurity response, and to promote stability in cyberspace through international co-operation. The Implementation Plan to the Cyber Declaration specifically envisages work on enhancing the protection of election systems through better cybersecurity.[16]

1.4 Relevant organisations and regulatory frameworks

There is a wide range of organisations whose work impacts or is impacted by issues of cybersecurity in electoral cycles, and these vary by Commonwealth country. Most clearly relevant is the EMB. As the public body with legal and administrative responsibility for the preparation and conduct of elections, issues concerning the integrity of the elections will usually fall at least partially within its remit.

Commonwealth countries distribute responsibility among government bodies for the electoral cycle in different ways. In some countries, such as *Pakistan* and *Ghana*, a central EMB has responsibility for most activities, shared between staff at a headquarters in the capital, regional offices and counting centres, and local polling stations. In others, such as the *UK*, a central EMB is responsible for party registration and spending controls, but hundreds of local authorities manage electoral registers and polling. In federations such as *Australia* and *Canada*, a devolved system to states may operate with a federal EMB. As well as national and local elections, many Commonwealth countries have important regional and provincial elections, and some have provisions for government or citizen-initiated referendums.[17]

Beyond electoral management bodies

There are, however, a number of reasons why **EMBs are not the only actors important to successful elections in a connected world**. In relation to some specific issues, they may not even be the main responsible bodies.

First, EMBs vary largely in **size, capacity and seasonality**. Many have few permanent staff, and instead adjust to variations through temporary structures and workforce in the run-up to elections.[18] Particularly in smaller countries, medium- to longer-term policy-making concerning elections is likely to more heavily depend on the co-ordination of an array of stakeholders across government – some of which may even be staff who would work for the EMB during an electoral period. There are also a number of non-permanent and not fully independent EMBs, this being applicable to a number of small states.

Second, electoral integrity extends beyond the direct electoral services provided by an election body to **wider societal and political systems,** with cybersecurity implications which might undermine the electoral process or trust in it. Examples of these include the cybersecurity of political parties or journalists; the use of automated systems for campaigning on social media; or the accumulation of campaigning funds through innovative digital financing mechanisms. In some countries, EMBs might face legal or practical restrictions around engaging with all relevant actors in the way cybersecurity issues demand: for example, for reasons of impartiality and transparency.

Third, the use of technology in and around elections is typically highly interwoven with the infrastructure, practices and **rulemaking of a range of public and private bodies.** Networked systems, such as the assets of internet and mobile providers and the services of social media and messaging providers such as Skype and WhatsApp, play important infrastructural roles. The hardware and software that public services operate on play significant roles in

cybersecurity issues, implicating the organisations and regimes that procure them. Many governments have unified systems for identifying citizens and use part of all of these infrastructures in different points of the electoral process. While some election bodies manage electoral rolls entirely separately from other parts of government, in many nations, the distinction is less easy to make. This can bring benefits – for example, highlighting when an individual has died by linking it to data used to inform other administrative systems; however, it also means that more collaboration is required.

Fourth, many issues concerning electoral integrity and cybersecurity **span jurisdictions**. Online platforms are particularly important, and many cross-jurisdictional issues regarding their responsibility across borders are currently playing out in legislative discussions and in the courts. This problem is heightened by globalisation in general, as voters are increasingly spread out across the world, and in many Commonwealth countries, overseas voters play an important and influential role in elections. Election bodies often have limited overseas reach, both in terms of their legal basis and their practical capacity, and may need to work in tandem with other bodies and even other governments in some cases.

The International Institute for Democracy and Electoral Assistance's (IDEA) *Cybersecurity in Elections – Models of Interagency Collaboration* publication outlines various different models of interagency collaboration which can be used to strengthen elections cybersecurity across governments. It is based on 20 case studies with EMBs and related government agencies from its network, in countries as diverse as Austria, Australia, Belgium, Bulgaria, Canada, Denmark, Estonia, Finland, Georgia, Latvia, Lithuania, Mexico, Moldova, the Netherlands, Norway, Romania, South Africa, Sweden, Ukraine, the United Kingdom and the United States.

The publication reflects that while adversaries are free to attack any part of a country's elections infrastructure, the state is often fragmented in its response. Responses differ across different national contexts, where the relative allocation of responsibility to the EMB, other state agencies, the private sector and parties will also vary across different threat types. Interagency collaboration is required to pool required resources and expertise; to develop better mutual understanding of areas of responsibility, overlaps and points of contact; and for building holistic defences against both domestic and international cyberattacks on elections and democracy.

In this context, the IDEA publication explores the following relevant questions:

- Which government bodies and private sector companies need to be involved?
- How should the collaboration of the various actors be structured, and what are their respective roles and responsibilities?
- How does co-operation work between different levels of the EMB and with non-state agencies?
- What formal frameworks – from legislation to memoranda of understanding – are required to enable, encourage and facilitate interagency co-operation?

The publication finds that it is easier for centralised EMBs to implement uniform cybersecurity measures throughout the country and that those with decentralised institutions will often bear the brunt of the criticism for cyberattacks, despite not having full operational control. Decentralised EMBs therefore need to place even more of a precedence on interagency collaboration.

The publication lays out the various levels at which multiagency collaboration can strengthen elections cybersecurity:

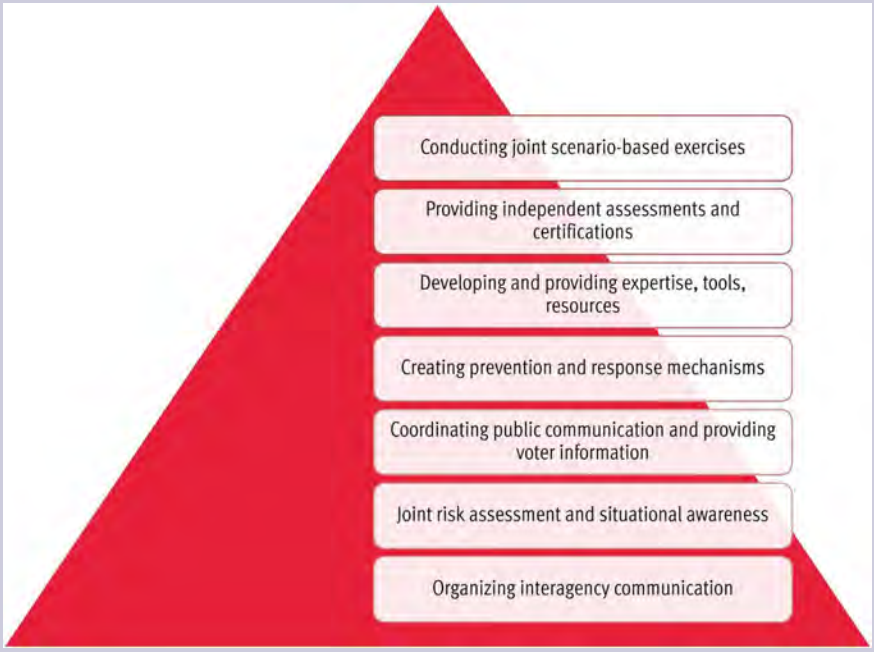


Figure 1.3 International IDEA's levels of multiagency collaboration

It also outlines a number of pertinent recommendations to enable and overcome the challenges to interagency collaboration:

- Interagency collaboration is a key element of improving resilience in elections. Electoral cybersecurity threats transcend institutional mandates. Tackling them often requires resources, information, situational awareness and expertise from multiple agencies. EMBs and other authorities working on elections should therefore consider the various models for interagency collaboration on cybersecurity, for example:
    - interagency communication protocols;
    - joint risk assessments; shared expertise, tools and resources;
    - independent assessments and certifications; and
    - scenario-based joint exercises
- To safeguard the independence of the EMB, any interagency collaboration should be publicly explained in a transparent and clearly defined manner.
- The private sector, political parties, academia, civil society and the media all play an important role in interagency collaboration, as do state agencies.
- International collaboration is needed, and election observers should assess domestic interagency collaboration.
- Designation of elections as critical infrastructure can help when interagency collaboration is absent.

Box 1.1 Models of interagency collaboration
Source: International Institute for Democracy and Electoral Assistance (IDEA)

Relevant regulatory frameworks

Many specific regulatory and policy regimes are relevant to electoral integrity. **Electoral law** outlines structural obligations and constraints on electoral processes, as well as permitting, prohibiting or mandating the use of particular technologies or data sources in elections. **Privacy** and **data protection laws** are in force in many Commonwealth countries. These are relevant in many respects, such as concerning the collection and processing of data relating

to voters and the private lives of candidates, and the use of digital marketing tools by campaigns (see Figure).

Figure 1.4 Ghana's National Communications Authority advertises its anti-spam SMS service

Also relevant are **laws concerning confidentiality of communications or correspondence**, which can implicate a range of digital signals and messages in an electoral context.[19] These sets of laws are particularly important in relation to data collected and used in the digital advertising and social media ecosystems, which are increasingly important campaigning grounds.

Cybercrime laws are also common. Several Commonwealth countries have signed and/or ratified a range of international cybercrime treaties,[20] and many have domestic cybercrime legislation.[21] These connect to laws governing the interception, collection and retention of digital **intelligence**, such as law regulating investigatory powers, which may be drawn upon by intelligence agencies, the police and other actors while investigating crimes, such as breaches of electoral law.

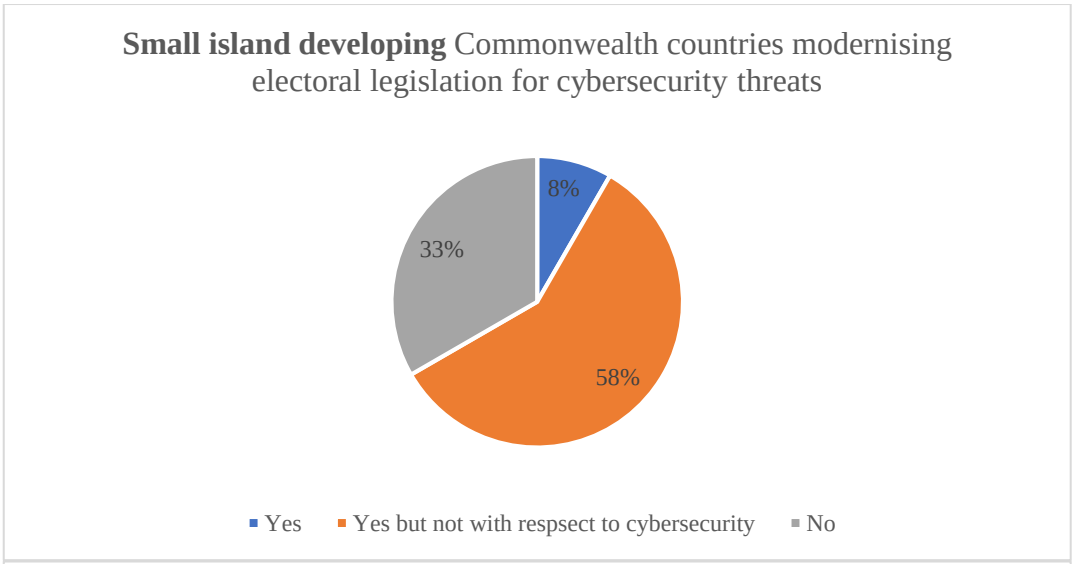
Ghana has acceded to both the Budapest Convention on Cybercrime (Council of Europe) and the Malabo Convention on Cyber Security and Personal Data protection (African Union), and it will soon ratify the former in parliament. Both conventions harmonise national laws, improve investigative techniques and increase co-operation between the parties in order to fight cybercrime, collectively improve cybersecurity and improve personal data protection. Ghana is one of only three countries on the African continent to ratify both conventions. It is also working directly with the Council of Europe through the GLACY+ (Global Action on Cybercrime) project, acting as a hub to support the capacity building of other states in the West African region.

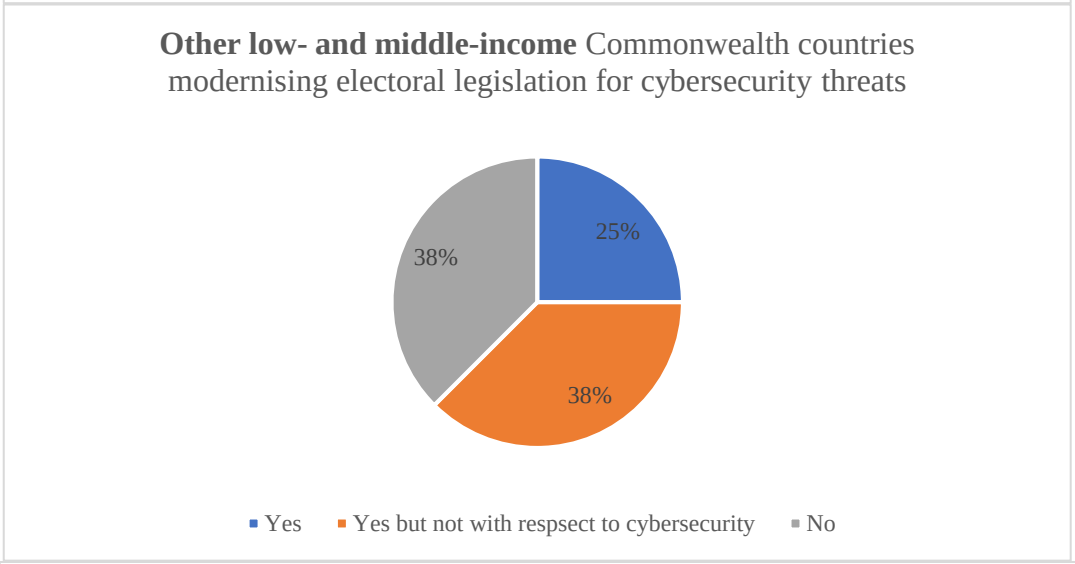
Box 1.2 International co-operation by Ghana

Public procurement law governs the way that public bodies of all types obtain digital technologies, and may place restrictions on which suppliers are eligible, their credentials or the ways in which governments can engage with them. Election bodies may fall outside of specific procurement rules for constitutional reasons, yet they are likely to be sharing or interfacing with infrastructure affected by such rules. Connected to this, **research and education policy** will affect whether a nation has specialists in cybersecurity, for example, in its universities and technical colleges, which in turn affects mechanisms of scientific advice to the public sector and the training pipeline for hiring experts.

Laws concerning **freedom of expression**, which often have a constitutional foundation, are important, particularly when read alongside **broadcasting law**, **media regulation** and **defamation law**. Many of these pieces of legislation are looked to regarding deceptive content online, such as fake accounts. Furthermore, **telecommunications law** governs the infrastructure that other electoral processes run on, such as results transmission or e-voting. Lastly, given the wide array of areas affected by digital processes, several nations have passed **omnibus 'digital-era' laws** to both update the regimes above and to create new regimes around them.[22]

Despite the importance of an up-to-date legal framework, only 15 per cent of respondent Commonwealth countries (see Figure 1) are modernising their electoral legislation to take into account cybersecurity and the prospects of foreign interference. The proportion is consistent across high-income, middle- and low-income, and small island developing countries.[23]





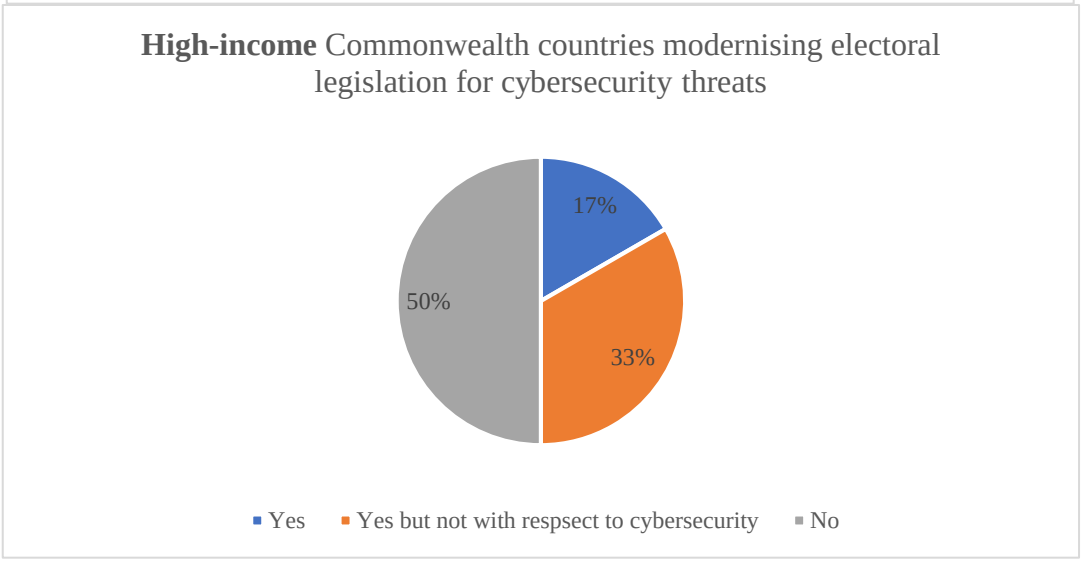


Figure 1.5 Proportion of respondent Commonwealth countries modernising electoral legislation for cybersecurity threats

Other relevant organisations

In general, responsibility for personal data protection, political advertising and media coverage, protection of telecommunications and other critical infrastructure, and investigation of electoral and cybercrime offences, lies with bodies beyond EMBs. A clear overview for all countries is not possible, as institutional structures can differ in scope or responsibilities, despite also sharing similarities. Some common groupings can, however, be located.

The National Cyber Security Centre (NCSC) of Ghana was established in November 2018 by a cabinet directive. Its remit is to co-ordinate cybersecurity across government, protect critical information infrastructure, raise awareness, provide incident response, set standards and facilitate public/private engagement. It currently employs around 20 staff and the World Bank is providing 3 consultants. Its institutions derive powers from Ghana's Criminal Investigations Division (CID), which has a mandate to investigate cybercrime. As part of the update to Ghana's cybersecurity framework, the NCSC will become an authority, in order to secure longer-term funding and better execute its mandate. It will also acquire further regulatory powers over the cybersecurity industry and critical sectors. including financial services, energy, telecoms, government sectors, health and – importantly – elections.

The NCSC is currently tendering for equipment and is in the process of setting up computer emergency response teams (CERTs) in telecoms, energy and financial services, to follow the central CERT launched in 2014. The first sectoral CERT was established by the National Communications Authority (NCA) for the telecoms/communications sector in October 2018. It is using the FIRST framework (Forum of Incident Response and Security Teams, a global association of CERTs) to provide services, including incident management, digital forensics, communications and outreach, capability development, research and development (R&D), and information assurance. It is working closely with the NCSC, particularly on incident management, in order to filter relevant intelligence to Ghanaian telecoms providers.

Box 1.3 Ghana's National Cyber Security Centre

Many countries have a range of **national cybersecurity actors**. Some countries have set up high-level organisations to co-ordinate cybersecurity capacity building and assurance in public functions, such as the *Australian* Cyber Security Centre, the *Canadian* Centre for Cyber Security, the National Cyber Security Centre (*UK* and *Ghana* – soon to become an authority) and the Cyber Security Agency (*Singapore*). Related to this, and sometimes independently or separately, countries often have cybersecurity strategy groups sitting under the executive.

In addition, at the time of writing, 29 Commonwealth countries were reported to have national computer security incident response teams (CSIRTs).[24] These organisations act as a co-ordinator and a point of contact for domestic and international stakeholders during an incident. Some of these have been established from scratch, while others have been elevated from existing areas of cybersecurity capacity within their countries.[25]

Trinidad and Tobago's National Cyber Security Strategy identifies a requirement for an organisation to serve as a national focal point for incident management. This was realised by the creation of the Trinidad and Tobago Cyber Security Incident Response Team (TTCSIRT) in November 2015, with the assistance of the Organization of American States (OAS) and the International Telecommunication Union (ITU). TTCSIRT is a Ministry of National Security unit, but the medium-term (five-year) plan in the national strategy is that it will be governed as an independent cybersecurity agency. This should help with perceptions of independence from government.[26] Its mission is to respond to cyber incidents, through effective response techniques, education, training, awareness, research, collaboration and efficient management strategies, in order to restore the operations of the information systems of Trinidad and Tobago.[27] TTCSIRT has primarily focused its operations on government networks, but will provide wider coverage over time.[28]

TTCSIRT plans to develop all of its own capabilities in-house by working with the police's newly established digital forensics unit. It has faced difficulties finding experienced staff, so is concentrating on training new staff. It has taken on two on-the-job trainees and will look at introducing three-month internships for university students. TTCSIRT only expects to keep staff for around three years, since their experience is so marketable. It can also take advantage of the

government's returning scholars programme, which gives graduates with a first-class degree funding for a master's degree (and in some cases, a PhD) in return for a year working afterwards.

Box 1.4 Trinidad and Tobago's Computer Security Incident Response Team (TTCSIRT)

Specialist police agencies also exist to support law enforcement capacity in these areas. One example of such a collaboration comes from *Mexico* in 2018, where the National Electoral Institute (INE) found a leaked copy of the entire electoral register on sale online. Together with the Special Prosecutor's Office for Electoral Crimes (Fepade), the Criminal Investigation Agency (AIC) and the Cyber Police, INE stopped the sale.[29]

Countries differ in terms of the location of their core cybersecurity expertise. In some countries, there may be significant public sector capacity and a range of in-house experts. Universities may form a core part of national expertise and may have training pipelines and world-leading research groups in areas of relevance to electoral cybersecurity and integrity. Yet in other countries, cybersecurity might not be a chosen national specialism for research and practice. In these cases, cybersecurity expertise might lie in sector-specific organisations, such as telecommunications or financial services companies, which may or may not be in public hands.

Independent communications regulatory agencies/authorities (CRAs) and ministries of information and/or communication have important roles in electoral cybersecurity. Election media coverage has cybersecurity dimensions and is a complex multiagency issue to regulate**. Political coverage rules** typically only apply to broadcast media, not print, online or outdoor posters. Those broadcast rules often apply to all broadcasting political coverage, with a 'fairness rule' and hate speech laws, with specific regulation of electoral periods. Yet with the continued increase in the use of multimedia in personalised online environments, this is fast changing the way political advertising works, creating new cybersecurity concerns.

Many regulators, including electoral, information and competition regulators, are considering the cybersecurity impacts of programmatic, **data-driven advertising online**.[30] The increase in highly targeted advertising, often selected using data obtained as a result of insecure transmission and brokerage,[31] both inside and outside electoral periods in online media, has been shown to be capable of causing disruption to electoral campaigning. The problem of hate speech has been shown to have causation with inter-ethnic violence and even genocide in both broadcast[32] and online media.[33]

All the above agencies are implicated in the new cybersecurity-related challenges to **electoral campaign regulation**. Media pluralism (ownership and content diversity) is a recognised and protected democratic value, contributing to the preservation and enhancement of electoral democracy, with a different stringency of regulation for different forms of media.[34] There is currently very little regulation of campaign activity on social media online in most Commonwealth countries, with no rules for content impartiality and limited oversight of campaign finance spending or of the ways automated systems (such as bots) might operate at scale. Where potential breaches of electoral law occur in the context of new media and technologies, the EMB may be forced to co-ordinate a multiagency response.

Twenty-two (22) Commonwealth countries are reported to have privacy and/or data protection laws (see Box 1). Some of these have associated regulatory bodies, such as the Data Protection Commission (*Ghana*), the Information Commissioner's Office (*UK*) and the Privacy Commissioner (*Canada*); meanwhile, other Commonwealth countries have laws without a regulator (e.g. *Saint Vincent and the Grenadines*) or have not yet appointed a regulator or commenced relevant parts of the law (e.g. *Barbados*, *Trinidad and Tobago, South Africa* and *Seychelles*).

Antigua and Barbuda	Kenya	Saint Lucia
Australia	Lesotho	Saint Vincent and the Grenadines

The Bahamas	Malawi	Singapore
Barbados	Malaysia	South Africa
Botswana	Malta	Tanzania
Brunei	Mauritius	Trinidad and Tobago
Canada	Namibia	Seychelles
Cyprus	New Zealand	Uganda
Dominica	Nigeria	United Kingdom
eSwatini	Pakistan	Zambia
Ghana	Rwanda	
India	Saint Kitts and Nevis	
Jamaica		

Box 1.5 Commonwealth countries with reported (or *proposed, limited or largely uncommenced)* data protection or privacy laws
Source: Commonwealth Secretariat

Some data protection authorities have seen significant budget increases in recent years to cope with changing legislation and changing issues. The *Cypriot* Data Protection Authority, for example, has reported an increase of budget by 70 per cent, between 2018 and 2019.[35] Such regulators and privacy frameworks may not reach to cover many parts of the electoral cycle, however, due to exemptions or a sole focus on public or private actors (see Chapter 3, in the section on '3.4 Privacy and data protection'.

Recommendation Governments should develop modernised laws and institutions to protect elections, addressing cybersecurity, cybercrime, data protection and telecoms/media regulation issues.

***

In sum, **contemporary electoral issues touching upon cybersecurity are broad and implicate a wide array of regulatory actors**. There is no 'best' institutional arrangement that will work across all national contexts, but these issues will require **new and strengthened forms of co-operation** across agencies that may not have worked together extensively before.

In the next chapter, this guide describes the **electoral cycle** and elaborates on cybersecurity-related challenges and emerging best practices within each element.

Notes and references

[1] Canada Communications Security Establishment (2019), '2019 Update: Cyber Threats to Canada's Democratic

Process', p.16.
[2] Jordan Robertson, Michael Riley and Andrew Willis (2016), 'How to Hack an Election', *Bloomberg Businessweek*, 31 March, available at: https://www.bloomberg.com/features/2016-how-to-hack-an-election/; one 'rotating group of 7 to 15 hackers brought in from across Latin America' allegedly 'worked on presidential elections in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala and Venezuela', charging between US$12,000 and US$20,000 per month.
[3] International Telecommunication Union-Telecom Standardization Sector, Recommendation X.1205, April 2008, p.2.
[4] Nir Kshetri (2016), 'Cybersecurity and Development', *Markets, Globalization & Development Review* 1(2), Article 3, p.3.
[5] Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization* 25(8), p.1405.
[6] Kim Zetter (2018), 'Was Georgia's Election System Hacked in 2016?', *Politico Magazine*, 18 July, available at: https://www.politico.com/magazine/story/2018/07/18/mueller-indictments-georgia-voting-infrastructure-219018
[7] Special Counsel Robert S Mueller, III, US Department of Justice (2019), *Report on the Investigation into Russian interference in the 2016 Presidential election*, p.4.
[8] See UNCTAD's UN official list of SIDS, available at: https://unctad.org/en/pages/aldc/Small%20Island%20Developing%20States/UNCTAD´s-unofficial-list-of-SIDS.aspx
[9] For example, in the Commonwealth, 35 per cent of respondent EMBs use biometrics such as fingerprints at polling stations.
[10] UK Electoral Commission (2007), *Electronic voting May 2007 electoral pilot schemes*, available at: https://www.electoralcommission.org.uk/sites/default/files/electoral_commission_pdf_file/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf
[11] Election Commission of Pakistan (2018), *Report on i-voting pilot test held in 35 constituencies on 14th October 2018*, available at: https://ecp.gov.pk/documents/ivotingreport.pdf
[12] The Commonwealth (2013), Charter of the Commonwealth, available at: http://thecommonwealth.org/our-charter
[13] Council of Europe Budapest Convention on Cybercrime, ETS No.185 (2001).
[14] Council of Europe (2018), Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
[15] UK Communications Act 2003.
[16] Commonwealth Secretariat (2018), Implementation Plan to the Cyber Declaration, available at: https://www.chogm2018.org.uk/sites/default/files/Commonwealth%20Cyber%20Declaration%20pdf.pdf
[17] See, for example, Recall and Initiative Act [RSBC 1996] Ch. 398 (British Columbia, Canada).
[18] See generally Toby S James (2017), 'Building Better Elections: The Role of Human Resource Management Practices', ECPR General Conference 2017.
[19] See, for example: in Malta, the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01); in the United Kingdom, the Privacy and Electronic Communications (EC Directive) Regulations 2003. See generally, the European Convention on Human Rights, Article 8 (everyone has the right to respect for [...] his correspondence'.
[20] See, for example, Council of Europe Budapest Convention on Cybercrime, ETS No.185 (2001); African Union Convention on Cyber Security and Personal Data Protection (2014). The Council of Europe's Cybercrime Convention Committee has produced a brief note on the application of its provisions to election offences in T-CY Guidance Note #9 – Aspects of election interference by means of computer systems covered by the Budapest Convention, adopted 8 July 2019.
[21] See, for example, Pakistan, The Prevention of Electronic Crimes Act, 2016, a law which does not flow from a treaty obligation.
[22] See, for example, the Digital Economy Acts (United Kingdom) 2010, 2017.
[23] As defined by the World Bank's Country and Lending Groups and the UN's classification of Small Island Developing Countries (SIDC) (World Bank, How Does the World Bank classify countries?, available at: https://datahelpdesk.worldbank.org/knowledgebase/articles/378834-how-does-the-world-bank-classify-countries; and UN Office of the High Representative for the Least Developed countries, Landlocked Developing Countries and Small Island Developing States, Small Islands Big(ger) States, available at: unohrlls.org/custom-content/uploads/2013/08/SIDS-Small-Islands-Bigger-Stakes.pdf).
[24] According to data from the International Telecommunication Union on national CSIRTs from March 2019, these are: Australia, Bangladesh, Barbados, Brunei Darussalam, Cameroon, Canada, Cyprus, Ghana, India, Jamaica, Kenya, Malaysia, Malta, Mauritius, New Zealand, Nigeria, Pakistan, Papau New Guinea, Rwanda, Singapore, South Africa, Sri Lanka, Tonga, Trinidad and Tobago, Uganda, the United Kingdom, the United Republic of Tanzania, Vanuatu, and Zambia.
[25] Robert Morgus, Isabel Skierka, Mirko Hohmann and Tim Maure (2015), *National CSIRTs and Their Role in Computer Security Incident Response,* GPPi (Berlin, Germany) and New America (Washington, USA).

[26] Ian Brown and James Lee (2019), Research Interview with TTCSIRT, December.
[27] Trinidad and Tobago Cyber Security Incident Response Team, 'Mission, Vision & Goals', available at: https://ttcsirt.gov.tt/index.php/mission-vision-core-values/
[28] Brown and Lee (2019), Research Interview with TTCSIRT, December.
[29] Melissa Galván (2018), 'El INE denuncia la venta en internet de una copia de la lista de electores', *EXPANSIÓN politica*, 7 October, available at: https://politica.expansion.mx/mexico/2018/10/07/el-ine-denuncia-la-venta-en-internet-de-una-copia-de-la-lista-de-electores
[30] Information Commissioner's Office (2018), *Democracy Disrupted? Personal Information and Political Influence*, ICO; Information Commissioner's Office (2019), *Update Report into Adtech and Real Time Bidding*, 20 June; Competitions and Markets Authority (2019), 'Online Platforms and Digital Advertising Market Study: Statement of Scope', 3 July.
[31] J Ryan (2018), 'Behavioural Advertising and Personal Data', Brave, available at: http://www.liguedh.be/wp-content/uploads/2019/06/Ryan-Report-original_.pdf
[32] For example, Rwanda in 1994, exacerbated by radio hate speech.
[33] For example, Myanmar in 2017, driven in part by Facebook group hate speech by religious leaders. See: Report of the Independent International Fact-finding Mission on Myanmar, A/HRC/39/64; *United Nations News* (2018), 'Myanmar military leaders must face genocide charges – UN report', 27 August, available at: https://news.un.org/en/story/2018/08/1017802. For a discussion of the commonalities in both genocides, see: Rita Franceschet (2019), 'Reflections on the Rwandan genocide 25 years later: Have we truly learned the lessons?', 6 April, Geneva International Centre for Justice, available at: http://www.gicj.org/positions-opinons/gicj-positions-and-opinions/1561-rwanda-genocide-25-years-lessons-learned-2019
[34] See, generally: Daithí Mac Síthigh (2018), Medium Law, Routledge (London and New York).
[35] European Data Protection Board (2019), *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, p.10.

Chapter 2 Cybersecurity across the electoral cycle

In electoral administration – even in the many Commonwealth countries that still use hand-marked paper ballots, manually counted, to determine the outcome of elections – computers and mobile devices have become indispensable tools to manage electoral rolls, delimit constituency boundaries, print poll books and co-ordinate the logistics of polling days. In some countries, they aid in collating and announcing results.

A smaller number of Commonwealth countries make greater use of technology in their interactions with voters during polling periods – to provide further checks of voter identity; to cast votes in person on electronic voting machines; and in some pilots, to allow remote e-voting.

Technology is even more pervasive when considering those participating in the electoral system more broadly. Political parties and campaigning organisations across the Commonwealth now make heavy use of voter data and social media to reach voters via direct marketing and targeted adverts, and of communications tools to internally plan and organise. In some countries, these forms of campaigning have partially displaced traditional campaigning. The *Canadian* government has reported that since 2015, the number of digital attacks on election infrastructure around the world has grown slightly, while attacks on political party cybersecurity and targeting of voters with disinformation have increased significantly:[1]

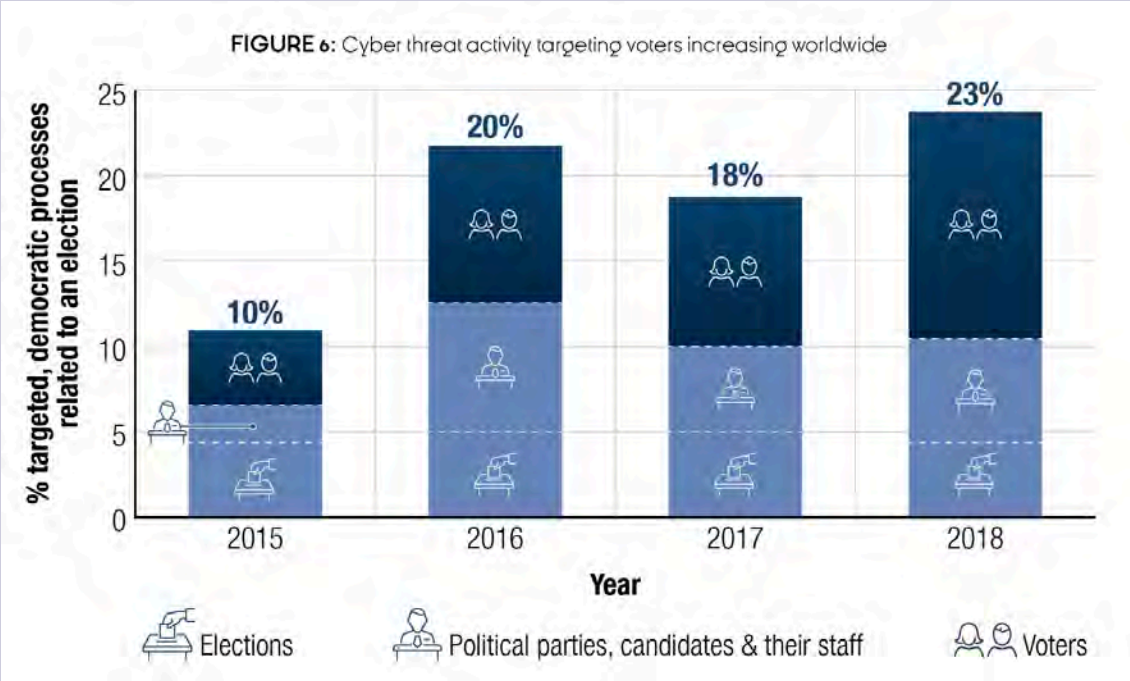


Figure 2.1 Cyber threats to global democratic processes, observed by Canadian Communications Security Establishment

The demand for data in political campaigns has led to practices that are arguably illegal in some Commonwealth jurisdictions and may more broadly betray voter expectations and confidence. There has been an increasing drive for detailed information about voters beyond that in electoral rolls. In some cases, such data have been obtained or processed illegally[2] or used in the context of high levels of microtargeting online, resulting in illegal electoral overspend.[3]

A regulatory response to electoral cybersecurity issues needs to include consideration of **direct threats**, emerging **vulnerabilities** and broader **systemic issues**:

- **Threats:** Attacks which undermine the confidentiality of information, the availability of systems or the integrity of processes *(e.g. attacks on voting machines or e-voting).*
- **Vulnerabilities:** Emerging practices which create new attack opportunities *(e.g. the use of electronic voter lists for online targeting by individual candidates using insecure devices).*
- **Systemic Issues:** Emerging practices which create new incentives for cyberattacks *(e.g. the increased demand for invasive datasets created by online targeting practices)* or a challenging environment *(e.g. a loss of public trust in technology).*

2.1 Election activities across the electoral cycle

A view of the election cycle from the International Institute for Democracy and Electoral Assistance[4] is shown in Figure 2.2. It is shown for illustrative purposes, as there is rarely such a clear separation between discrete phases of EMB preparation. To take one example, updating electoral registration is an ongoing process that is often most intensive in the immediate pre-polling period. In the digital era, campaigning also continues throughout a parliamentary term, with online messaging from registered parties and, increasingly, by single-issue causes not formally aligned with parties.

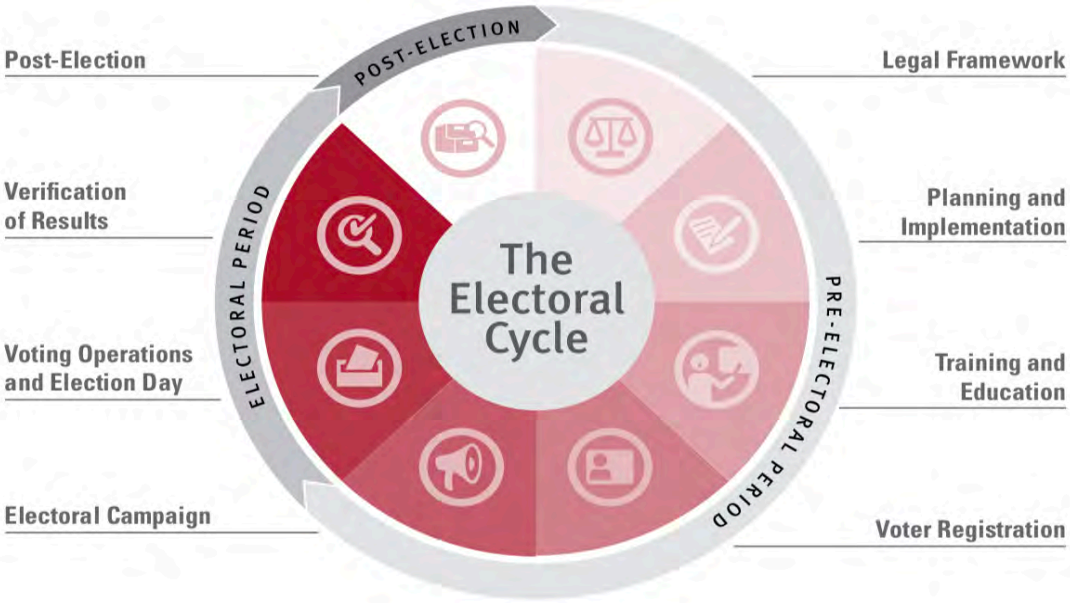


Figure 2.2 The electoral cycle as presented by International IDEA

We have therefore used five categories of activities which help explain the overlapping sequencing of EMB preparation and operation: [1] planning and logistics, training and education; [2] electoral registration; [3] campaign regulation; [4] vote counting, verification and reporting; and [5] post-election audit and challenge. The first two categories are perpetual roles for EMBs: logistics and registration are never-ending processes. Furthermore, post-election challenge includes a 'post-mortem' by EMBs, parliamentary authorities, and ministries of justice and equivalent, even where there is no significant legal–judicial challenge to the electoral process. The legal framework is updated as a response to challenges discovered during electoral processes, as well as encompassing international best practice (as, for instance, from this guide).

Some of the different activities within this cycle that are vulnerable to cybersecurity threats before, during and after voting are shown in Box 2.1.

	Pre-polling	Polling	Post-polling
Planning and logistics; training and education	Boundary delimitation Polling station placement Recruitment of polling station staff Candidate/party registration/education Procurement	Disseminating logistical information Disseminating electoral materials	Retrieving results and electoral materials Analysing delays and other issues in specific polling locations Preparing election teams for future
Electoral rolls and registration	Compiling rolls Checking for ineligibility or duplication Adding/verifying voters Setting dates for final pre-election registration Co-ordinating with local authorities (where necessary)	Verification of voters Electronic voter roll systems Providing unverified voters with appeal mechanisms/process information	Domestic and overseas turnout calculation Assessment of issues in vulnerable communities based on surveys – e.g. disabled, minority, indigenous, rural groups Response to individual voter concerns and complaints
Campaign regulation	Enforcement of campaigning rules online Oversight of electoral rolls provided to candidates and parties. Monitoring for fake electoral information	Monitoring inappropriate restrictions of information, such as internet switch-off Monitoring and reporting of electoral incidents at polling stations	Reporting of all electoral competences, such as campaign spend
Vote counting, verification and reporting	Postal vote tallies, summary data and verification Registration of proxy voters or special arrangements Standards for results feeds to media and individuals	Ensuring secure voting machines and infrastructure Ensuring functional verification Tabulation and transmission Ensuring integrity of backup procedures	Investigation of electoral abnormalities Maintaining secrecy of ballot, for example, internet voting Securely aggregating votes, for example, by district. Using results for future planning
Audit and challenge; legal reform; best practice adoption	Citizen/candidate facing verification of registration	Compromise of observers, monitoring and observation systems Counteracting disinformation about logistics	Case management system for electoral irregularities Electoral court, recall of candidates

Box 2.1 Aspects of the electoral cycle vulnerable to cybersecurity risks

2.2 Overarching features of direct threats

At a technical level, cybersecurity attacks are usually concerned with:

- breaching the **confidentiality** of systems and exposing information to those not intended to see it;
- undermining the **integrity** of systems and disrupting the accuracy, consistency or trustworthiness of information being processed; and/or
- affecting the **availability** of systems and rendering them offline, unusable or non-functional.

All of these characteristics or attacks might play out in an **indiscriminate** manner (e.g. revealing, corrupting or disrupting all information and systems) or in a **targeted** manner (e.g. only leaking data from certain candidates or disrupting systems in certain locations). An example of a targeted confidentiality attack can be seen in Box 2.2.

During the 2016 US presidential election, a large volume of confidential email messages was stolen from the Democratic National Committee and later published via WikiLeaks, by what the US intelligence community assessed was the Russian military intelligence agency GRU. Some of the messages were so embarrassing to senior party staff that they resulted in resignations, angry recriminations between supporters of candidates Hillary Clinton and Bernie Sanders, and weeks of negative media coverage. The same group successfully infiltrated systems of the Illinois state election board, stealing 'information about 500,000 voters, including names, addresses, partial Social Security numbers, dates of birth and driver's license numbers'.[5]

Box 2.2 Targeted confidentiality attacks on political parties and campaigns

Because the internet is a global network, attacks can come from anywhere, with their origins disguised. Even well-managed systems with regularly updated software and the careful use of security tools such as firewalls and anti-virus software can be vulnerable. Attackers are constantly finding new weaknesses in software and systems that allow them to gain unauthorised access, to read and even change data, or to block access to the systems by authorised users. Attackers also look for opportunities to find and even introduce weaknesses into components and systems supplied to electoral authorities, with one *USA* intelligence report stating:

> Russian General Staff Main Intelligence Directorate actors … executed cyber espionage operations against a named U.S. company in August 2016, evidently to obtain information on elections-related software and hardware solutions. … The actors likely used data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations.[6]

The report concluded that data obtained from an e-voting vendor would be used to trick local government employees into opening infected documents that would enable full, remote control of those computers.

All parts of the modern electoral cycle are characterised by a complex set of networked applications, systems and infrastructures. Electoral systems interface directly and indirectly with other national and international infrastructure, from ID databases to office software, all of which are increasingly managed in modular ways, with data flows and software updates which are difficult to monitor.[7]

Electoral systems are so important, they are likely to be candidates for targets using types of attacks that normal businesses may not face. In 2018, the European Council expressed 'serious concern about the increased ability and willingness of third countries and non-state actors to pursue their objectives by undertaking malicious cyber activities'.[8] This means that cyber-defence strategies that are adopted routinely by normal business actors are unlikely to suffice for critical electoral systems.

For example, while systems are particularly vulnerable to attack when they are connected to the internet, 'air-gapped' systems (which are physically isolated from unsecured networks) are not immune to threats. They may still be accessed physically – by authorised staff or in

polling stations, by voters – or compromised by pre-installed software or update processes. Such attack forms are more costly, but are unlikely to deter a determined state actor.

As electoral systems are valuable targets, they also require readiness for the use of costly technical attacks. So-called *zero-day vulnerabilities* are named as such because the vendor or system designer has zero days of notice: this will be the first time they have seen this particular bug or loophole being used. Zero-day vulnerabilities are valuable for attackers and hoarded by state actors, and are mostly only used for attacks with high potential payoffs. For some attackers, these might include key democratic processes and critical infrastructure. Similarly, hardware attacks by state actors might make use of foreign control of manufacturing and supply chains and the difficulty of checking systems such as computer chips for hardware designed to leak information or compromise systems.[9]

Yet both state and non-state actors can engage in electoral interference. It does not require sophistication, technical expertise nor access to resources to procure cybercrime services in online marketplaces, where malicious actors can obtain the means to carry out distributed denial of service (DDoS) attacks (the malicious flooding of web traffic from multiple sources to overload a system and prevent legitimate requests from being fulfilled) and malware (malicious software, including computer viruses, worms, trojan horses and spyware, among many others).

EMBs should plan particularly carefully for the cybersecurity of systems that will be used during and in the immediate run-up to elections, when successful attacks can be especially damaging. They should consider pausing non-critical software updates and patches in this period.[10]

Insider threats

Organisations must carefully consider cybersecurity threats from 'insiders' – staff, candidates and volunteers with authorised access to systems, both within political parties and within organisations such as EMBs or contractors. Political parties may be at risk of campaigners or splinter organisations acting alone and potentially illegally, such as the disinformation campaign based on stolen voter data seen in *Canada* in 2011 (see Box 2.3).

During and following the 2011 Canadian elections, Elections Canada, received a range of complaints concerning phone calls voters had received containing misleading information, including about the location of polling stations. These automated phone calls – or 'robocalls' as they are commonly called in North America – impersonated officials from the EMB and were accused of claiming that the location of polling stations had been moved due to incorrect estimations of voter turnouts. The addresses given of these polling stations were fictitious, and indeed Canada's EMB does not use phone calls to contact voters at all to tell them about incidents such as these.

The Federal Court concluded that the phone numbers and voter contact information were taken from a database developed and maintained by Canada's Conservative Party, and ruled that in the six districts that the complaints made concerned, these calls did meet the statutory definition of voter fraud. While the judge could have annulled the disputed results, which were in swing seats, he chose against this due to lack of evidence that the fraud had sufficiently affected the results.[11] Related to this, a campaign worker for the Conservative Party was sentenced to nine months of imprisonment and twelve months of probation for violating the Elections Act by engaging in voter suppression through robocalls.[12]

One challenge raised by this case is that the plaintiffs had the burden of proving that the cybersecurity-related electoral integrity breach cause a swing in the votes. While the plaintiffs took the unusual step of an automated survey – a robocall to assess the impact of a robocall – to ask citizens about their experiences, the judge was unconvinced.[13] EMBs must be ready to examine complex situations for evidence of the impact of cybersecurity breaches if and when they occur.

Another issue relates to the use of the datasets internally by campaign workers. Insofar as the use of the datasets in this way was illegal, it is important to consider what obligations parties have to secure their datasets against internal threats. Courts in the United Kingdom are currently assessing the extent to which the organisation holding the data, such as a political party, can be held vicariously liable for similar breaches.[14] However, as discussed, political parties are not clearly governed by privacy law in Canada and so this issue did not arise in the *robocalls* case.

Box 2.3 Canadian 2011 robocalling scandal

Insider attacks cannot always be totally mitigated, but it is important that such threats are modelled and considered both within and around EMBs and in political parties. EMBs must be aware, model and seek to mitigate risks of bribery and corruption, particularly as salaries for IT professionals in the public sector are often significantly lower than those in the private sector.

EMBs should work closely with existing efforts to secure government data against insiders, such as undertaking anti-fraud programmes (run by both public and private actors), should use restrictive access controls where possible and advise political parties to limit data access to only those who need it. In some cases, non-disclosure agreements with former workers in sensitive positions may also serve to help limit dissemination – although these should not be used to limit disclosures of security lapses by whistle-blowers.

In *South Africa*, the EMB asks the state security agency to vet key appointments, on an advisory basis. In *India*, people with direct database access are felt to be most security-critical and database administrators (DBAs) are subject to the highest level of security vetting. For security-critical functions, two DBAs must approve changes, while employees must also sign long-lasting non-disclosure agreements (NDAs).

Recommendation 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.

Recommendation 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.

Maintaining trust

Attacks on elections can be designed to undermine the trust in electoral systems. Furthermore, regulatory responses themselves to both technology and cybersecurity issues must navigate issues of public trust.

Many of these forms of attacks are indiscriminate, intending to *disrupt* rather than *manipulate* the outcome of an election, targeting areas such as voter registration or the release of results. Common current attacks of this type affect election agency websites. In carrying out these activities, foreign adversaries generally attempt to sow doubt about the validity of an election result, rather than covertly change the result itself.[15] Even targeting a single area of a constituency can sow doubt as to the integrity of broader election processes.[16]

The consequences of intrusion, alleged or otherwise, can be highly damaging to public trust. For example, one Commonwealth country in Africa had to re-run presidential elections following allegations that the Elections Management System (EMS) and results transmission mechanism had been compromised, together with an annulment from its Supreme Court which found that the poll was 'neither transparent nor verifiable'. At least five people were killed in protests following the allegations by the opposition leader.

The independent status of many Commonwealth EMBs can also make it more difficult for them to make wider use of national government cybersecurity infrastructure and expertise. Even collaboration with a government cybersecurity agency may provoke suspicion, as many are associated with intelligence agencies.

The reliance on third party vendors can complicate matters further and pose supply chain and reputation risks that EMBs will need to carefully manage. Extensive reliance on foreign vendors or auditing bodies may provoke allegations of electoral interference by powers with access to these supply chains, which may be warranted or unwarranted.

Recent experience suggests that [election] technology relies on complex procedures that are liable to break down, may actually increase popular suspicion of manipulation, and encourage complacency towards traditional forms of election oversight. Given this, when considering which types of digitization are worth the cost, it is important that greater attention is paid to the limitations and unintended consequences of these new methods.[17]

A key requirement in maintaining public trust while introducing new electoral technologies is to ensure that fall-back processes are available if technologies fail during an election. For example, if voter verification devices cannot successfully authenticate one or more voters, how can officials in polling stations do so, even at a slower pace? If results cannot be transmitted directly by results transmission systems (RTSs), can secure messaging apps on officials' phones be used as a fall-back? And what are the security implications – and potential impact on voter confidence in outcomes – of using such systems? How can the use of these systems be observed and audited?

2.3 Planning and logistics

Ancillary IT systems are routinely employed in the planning and logistics phase of the electoral cycle. These include:

- geographic information systems (GISs) to delimit constituency boundaries; and
- modelling and aggregation tools to monitor demographics, such as population change.

These tools can inform changes such as to constituency boundaries, with significant electoral consequences. As a result, there is potential for attackers to undertake subtle manipulation of the data and results. This might happen through **changing the logic of the analytic systems being deployed** or by **compromising points in data collection, cleaning, processing and storage**.

There is (usually) a long timeframe during which the changes are publicly debated, and hence attacks on the integrity of these outputs have time to be detected before they become implemented. However, it is more likely that such attacks would seek to undermine trust in the process rather than integrity of the eventual legally binding decision. This might also occur through, for example, leaking of confidential discussions, such as releasing calculations or drafts early to create public controversy, or by providing a misleading impression of a decision process. In general, the high politicisation of re-districting in some countries could result in these interventions causing heavy damage to public trust.

Recommendation 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.

In the run-up to elections, **systems can also be used to support shorter-term decisions such as the location of polling stations, delivery of ballot papers, and management of staff and volunteers.**[18] There is a greater risk here of successful attacks causing problems to the smooth running of the elections. These systems may be deployed without the knowledge of an EMB, for example, if it utilises the services of a logistics contractor who draws upon decision-support software, which itself has not been directly procured by the EMB.

Recommendation 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.

Many Commonwealth governments can call 'snap' elections, and as a result EMBs may not have the lead time they expected to organise elections, including to assess and mitigate cybersecurity risks. EMBs should therefore seek to make cybersecurity threat assessment and mitigation efforts a part of their ongoing work, undertaken with more regularity than electoral cycles.

Recommendation 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.

One innovation concerning electoral rolls is the SMS service the Election Commission of Pakistan created to help citizens check their status in electoral registration: in particular, their electoral area, block code (with which they can refer to further documents to find their polling station) and serial number. Citizens text their national identity card number to 8300, and this information is returned (from any telephone). The database underpinning this service is not connected to the internet, but on a separate circuit switched device. It was unclear whether the access to this data on the basis of a national identity card number would be useful to adversaries, although data such as a serial number is partially redacted when returned by SMS. This service received an award at the International Parliamentary Organization's International Electoral Awards 2013.

Box 2.4 SMS look-up of polling station location in Pakistan

Almost all Commonwealth countries require voters to visit a polling station on a specific election day or days to cast their vote – either at a particular location, based on their home address, or in some countries (such as *Australia*), a polling station within their constituency. (Some countries allow a significant fraction of the population to cast a postal vote over a longer time period). Most countries notify voters of their allocated polling station by post, with some (such as the *UK*) enabling voters to look this up via a website or by mobile phone text message (for example, *Pakistan,* see Box 2.4) and even digital assistant (*Barbados*).

Electoral agencies generally have a duty to provide, or support, public information campaigns prior to elections to drive voter registration, and within elections to encourage voters to exercise their democratic rights. In this specific area, disinformation can act to prevent the electoral authorities' message of enfranchisement from being clearly communicated to voters. Where false information is deliberately used to confuse or prevent potential voters from registering (including for residential immigrants and expatriate voters, where applicable), this can be a serious criminal offence. Disinformation can be used to convince the politically unattached to remain apathetic and not register to vote, or in any case to cast a vote. Suppressing voter turnout can be an effective political strategy and laws in, for instance, the *United States* have targeted voter suppression techniques.

If information services provided by EMBs are hit by a denial-of-service attack, or false information returned, this could reduce the turnout of affected voters – perhaps in areas known to favour specific parties. There have been cases where disinformation has been spread online or by automated calling about the location and timing of polling stations (see, for example, Box 2.3 on *Canada* and robocalling, above), and of the eligibility of groups of voters more likely to vote for specific candidates.

Recommendation 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.

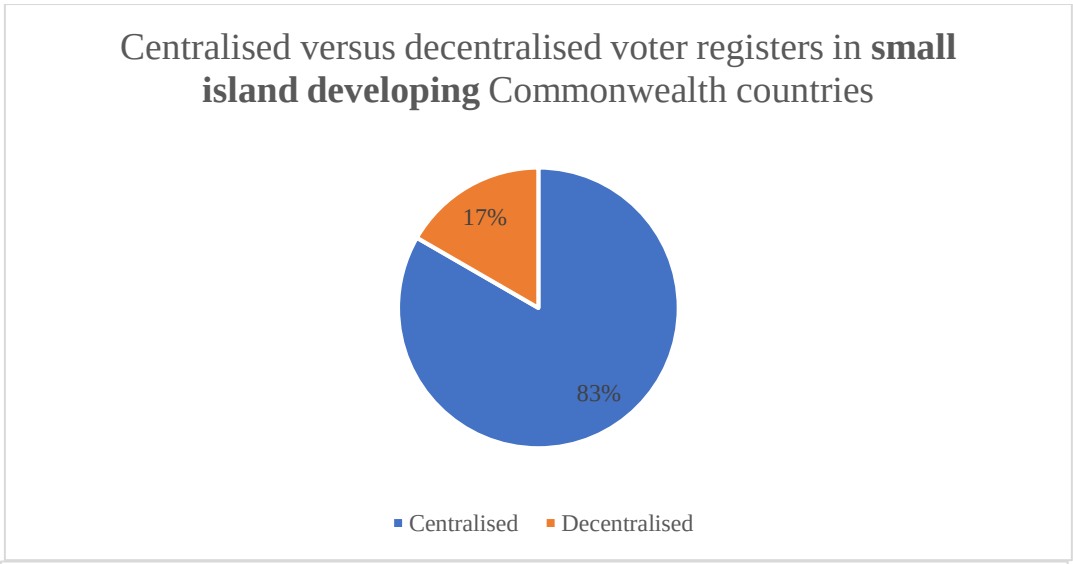
2.4 Electoral rolls

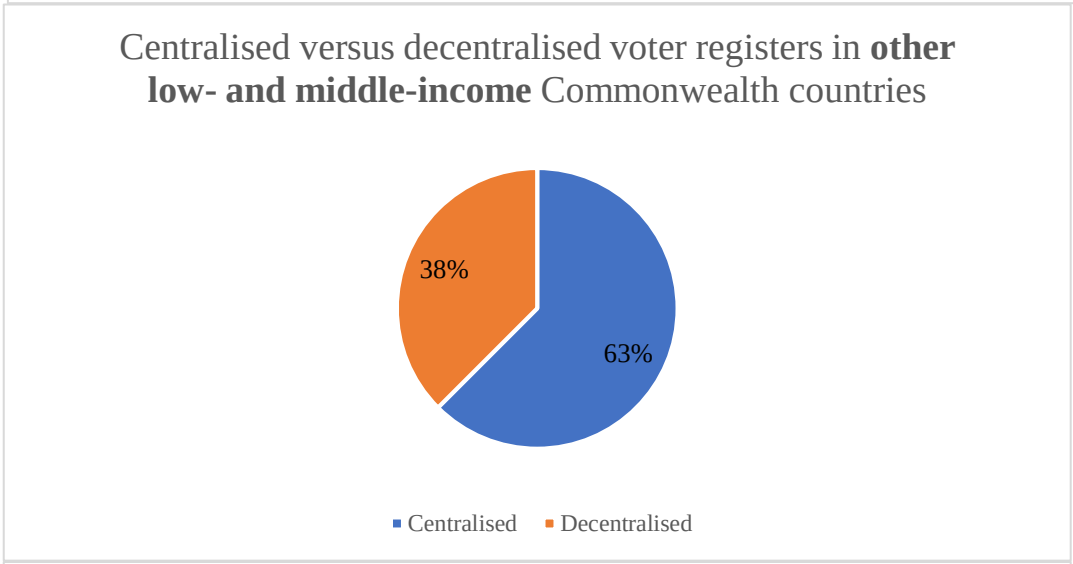
Democracies' electoral registers list all eligible voters and also inform broader administration and planning questions for polling days, such as how many voters to expect at each polling station.

Registers are managed in different ways. In some Commonwealth countries, the electoral registration process is separate from other government tasks (e.g. the *UK*), where it is the voter's responsibility to register themselves anew when they move or become eligible to vote. Some countries operate mixed systems. In *Canada*, voters can choose to opt out of the shared electoral list at the cost of having to register before each election directly. European Union member states, such as *Malta* and *Cyprus*, have an opt-in system due at least in part to the potential for European citizens to register to vote in local or European elections in the member state in which they reside. In *Pakistan*, data from the national ID system is used to populate the electoral roll, although this is done using two separate systems, with the EMB

having specific responsibility for the electoral roll and permitted to make changes which diverge from general government databases.

Furthermore, different members manage electoral rolls at different devolved levels. Some Commonwealth countries give significant authority for roll management to local entities, such as *Bangladesh, Cameroon* and the *UK*, while others, such as *Botswana, India* and *Solomon Islands,* take a more centralised approach. Seventy-seven (77) per cent of the respondent Commonwealth countries adopt a centralised voter register. Figure 2.3 shows the full breakdown across high-income, middle- and low-income and small island developing countries. A national registration database may populate local databases at regular intervals, local databases might be compiled into regional or national databases, or there can be a mixture of both systems.[19]





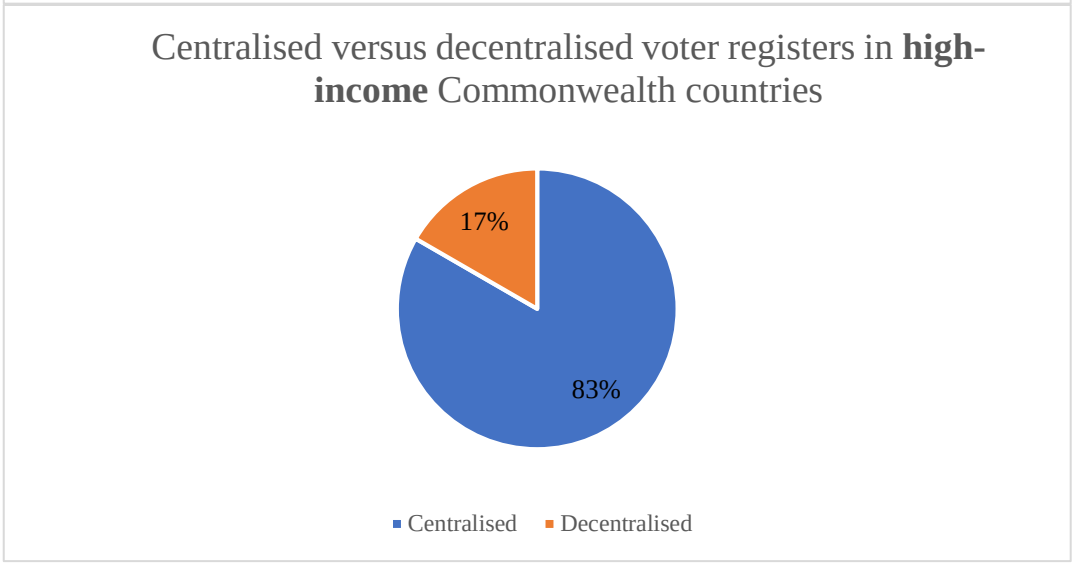


Figure 2.3 Centralised vs decentralised voter registers in respondent Commonwealth countries

In many Commonwealth countries, copies of the electoral roll are legally permitted to be provided to *bona fide* campaigns, parties, candidates and representatives. In some members,

this roll is open to scrutiny from the public in designated locations, such as local authority offices, and those on the roll may have opted in or out from a commercially available version of the register.

Political parties are potential cybersecurity targets due to their privileged access to voter data. For example, in the *UK*, parties and relevant third parties are eligible for copies of the electoral register for electoral purposes.[20] Similar provisions exist in *Australia*,[21] *Canada*[22] and *Pakistan*,[23] among many other Commonwealth countries. These datasets, containing the names and addresses of the majority of citizens, are of high commercial value and potential sensitivity, and there are often, but not always, significant restrictions related to their downstream use by political parties.[24] Consequently, they are valuable targets.

Insider leaks might also involve candidates using voter data illegally – for example, as was seen in *Canada* where party databases were abused to run automated calls to voters impersonating an electoral authority and providing false ballot booth locations (see Box 2.3, above. In other countries, the electoral register is a public document – in *Ghana*'s case, it is available on the EMB website – but confidential voter information, particularly biometric data such as fingerprints, is not included. *Grenada* makes the electoral roll available online, copied quarterly from the EMB's secure hosting system to the web-accessible system. *Antigua and Barbuda* has allowed e-registration since 2013 and publishes the register biannually via its website.

Defending against attacks on the confidentiality of the register is made particularly challenging when the roll is not only in the hands of the EMB and, consequently, it may be at its most vulnerable further downstream. *Mexico*'s Instituto Nacional Electoral (INE) filed criminal charges after an unprotected database of 90 million voter registration records was found hosted on Amazon Web Services. The institute suspected the data had been leaked by one of the political parties, which are given copies.[25] An investigation showed the database had been accessed 2,400 times from 14 internet protocol (IP) addresses.[26] The national Electoral Court fined the *Movimiento Ciudadano* party and two individuals 34 million pesos (£1.4m) for the leak.[27]

To limit the opportunities for misuse of electoral registers, some Commonwealth countries limit the information that is made public. In *Malaysia*, only the last four digits of voters' national identification numbers are included in the published register. In the *UK*, voters can opt out of their records being included in the full public register, appearing instead only in a restricted register used for election purposes and a limited number of other functions, such as credit referencing. They may also object in writing to political party use of their data.

In *India*, there has been controversy over the publication of a machine-readable form of the register, which already has voter photos and home addresses removed. In *Antigua and Barbuda*, the law has blocked police requests for use of the EMB fingerprint database. Following the 2015 leak in Mexico, the INE limited the information shared with parties to the names of registered voters. The investigation of that leak was aided by the inclusion of 'fingerprinting' data in the copy of the register shared.[28]

Where the law allows voter registers to be provided to a political party, it often also allows it to be provided to a candidate independently. This is important for ensuring that non-affiliated candidates without parties can operate on a level playing field in an election with larger political machineries. However, such individuals are unlikely to have the capacity required to secure data to an acceptable level and may be more vulnerable to 'phishing' and other attacks aimed at stealing these documents. Some Commonwealth countries, such as *Pakistan*, seek to limit threats such as these by only distributing the register to candidates in paper form where possible, therefore limiting its existence in digital form.

Commonwealth countries without data protection or privacy laws which apply effectively to political entities (see Chapter 3, section 3.4 Privacy and data protection, and Box 1.5, above) are in a particularly challenging situation, as these entities may not have sufficient incentives or expertise in security practices in order to protect provided data more generally. Where there is a detected breach, there may be no obligation to report to a regulator or to the EMB, and thus no opportunity to manage the potential electoral fallout that might result. Without

clear data breach reporting requirements, it is also highly possible that a breach may not be detected by the organisation in question.

Recommendation 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.

Recommendation 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.

Electoral rolls can become highly politicised, and as a consequence ensuring their integrity is of paramount important to the integrity of the election as a whole.

Issues around the integrity of electoral rolls predominantly concern:

- the **addition** of non-eligible voters;
- the **non-removal** of non-eligible voters (e.g. the deceased or duplicate records); and/or
- the **removal, failure to register** or record **corruption** of eligible voters.

This might happen in ways that are targeted to disrupt the election, such as in swing regions, or to enable a specific pattern of voting fraud, or it might happen in an indiscriminate manner designed to undermine trust in the electoral roll and the EMB more generally.

Some Commonwealth countries check electoral roll data against government datasets such as central population registries, births and deaths or tenancy records in order to remove ineligible voters or for auto-enrolment purposes. One electoral observer told us: 'There are some countries where the range of datasets being used to compile the register is so vast that there are long discussions about what takes precedence when there is an apparent conflict. Often this results in a political decision being taken to seek to benefit one party or another'.

National digital identities are becoming the basis of electoral rolls in some Commonwealth countries, such as *Pakistan* (see Box 2.5). *Mauritius* has an annual household door-to-door canvas, and the Ministry of IT has designed an 'information highway' to link government agencies, which the EMB can use to check registrations against the civil registry. *South Africa* has a national population registry managed by the Ministry of Home Affairs and each citizen is issued with an identity number at birth. Hospitals report births and deaths, while access to all public services requires an ID number. For registration, the ID number is collected through the use of an electronic device and the details and citizen status of the person checked against the national population register. Voter registration is voluntary, but checked against the population registry, and voters can verify their registration online (via website, SMS and/or an app) and check their polling station details. Voters can also view and change their address details online.

While the *UK* does not have a national identity scheme, its Electoral Commission is exploring other mechanisms for automatic voter registration.[29] Elsewhere, in *The Netherlands*, local municipalities maintain a population register which includes each resident's right to vote. This is used to send every eligible voter an invitation to vote before each election, along with details of their polling station.[30]

Pakistan's National Database and Registration Authority (NADRA) has supported the Election Commission of Pakistan to verify unique voters via the National Citizen Database. Following political controversy surrounding the electoral roll, computerised national identity cards (CNICs) (which have 100 per cent coverage of all Pakistani households) are now required to vote. NADRA currently hosts the electoral roll, although the Election Commission is seeking to migrate from NADRA premises and gain infrastructural oversight given the constitutional independence of the electoral system. In terms of external attacks, NADRA is predominantly concerned about defending the integrity of the data from foreign actors, particularly those who want to insert fake data into the database – a concern that aligns with that of the Election Commission.

Box 2.5 Electoral roll integrity in Pakistan

These approaches bring trade-offs that need to be carefully navigated. They may increase the integrity of the electoral roll through data cleaning and validation exercises. On the other hand, they increase the opportunities for successful attacks, as there are more data sources feeding into the electoral roll processes, and an undetected loss of integrity in any of these systems may result in a loss of integrity in the roll more generally.

Attempts to avoid fraud in the electoral roll might end up disenfranchising voters. The infamous *United States* 'Crosscheck' system was used to strike off alleged fraudulent voters, until the system was stopped from operating in certain parts of the US on the basis of an injunction from a Federal Court amid concerns about its constitutionality.[31] And a number of African opposition parties have alleged that governments have made it harder for their supporters to obtain national identity documents or otherwise register to vote, by locating registration centres far from areas where they are most popular.[32]

Recommendation 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.

Recommendation 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.

Recommendation 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.

Availability issues might affect registration systems for voting, voter validation systems (for example, the SMS service operated in *Pakistan* to allow voters to check their registration status) or the availability of parts of the electoral roll for downstream processes, such as the creation of pollbooks.

The frequency and means of update to the electoral roll varies significantly across Commonwealth countries, with particular consequences for expectations of availability. Registration methods include automatic, in-person, post, fax and online. The *UK* provides a Register to Vote website,[33] which sends a completed form to the applicant's local Electoral Registration Officer to add to the electoral roll once the application has been validated. *South Africa*'s 1996 Constitution required a national common voters' roll to be created quickly. The Electoral Commission scanned voters' identity document barcodes and used this to retrieve name and voter status from the National Population Register. In only six days, 18.1 million of the 18.4 million applicants were successfully enrolled.

Electronic pollbooks might promise same-day registration, even up to polling day, but such expectations of immediacy can amplify the effects of any availability attacks, which might scupper citizens' last-minute attempts at registration. The *UK* was affected by an availability incident shortly before an extremely controversial referendum (see Box 2.6), which led to public concern and parliamentary action to change the voter registration deadline.

The UK saw a highly publicised availability incident in 2016, as the voter registration system was unavailable prior to the deadline. The parliament stated that the loss of functionality of the election registration system just prior to the deadline during intense public demand had 'indications of being a DDoS [distributed denial of service] "attack"', although government agencies called it a 'self-DoS'. Because the vote was a referendum and not a general election, parliament was sitting and, as a result, could vote to extend the registration deadline. If this had been a general election, parliament would have been dissolved and could not have extended the deadline in such a manner, with unclear implications for the vote.

Box 2.6 Voter registration and availability attacks in the UK

Recommendation 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.

Recommendation EMBs should prepare and practise backup procedures where availability attacks on critical systems might disrupt electoral processes.

2.5 Campaigning

Political parties are increasingly taking advantage of the highly targeted advertising capabilities offered by social media platforms to share their election messages, but are also following their potential voters – who across the Commonwealth, spend increasing amounts of time online. One significant challenge concerning online campaigning surrounds the **systemic incentives for insecurity** built into online advertising infrastructures today.

Advertising online is primarily carried out on the internet and on mobile applications. In both, there is a range of more 'open' advertising opportunities, such banner ads, which any website or application can embed within its service; and advertising on closed platforms controlled by a few concentrated market actors, such as Facebook, Twitter or Google, which are displayed within those platforms. Both types of campaigning are highly data intensive.

General targeted advertisements are often run through a process called 'real-time bidding', which consists of an auction for ad placements that is programmatically executed in the milliseconds before a webpage or app loads an advert. This process, in short, sees a browser or application transmit data about the user to an advertising exchange, which passes it on to hundreds or even thousands of agents working for a potential advertiser. The task of these agents is to assess whether the person is 'worth' spending the money to deliver the advert to – for example, if they are likely to click on it or spend time viewing it. To do this, they use a process called '**enrichment'**, where the data provided to advertising platforms is passed to a 'data management platform' – whose job it is to combine amassed data of their own, prediction systems and the data of customers (such as political parties) together.[34]

This data management platform – an example of which is Cambridge Analytica (see Box 2.7) – will cross-reference the device data with their own data, and provide a profile back to the advertisers' agent, who will place a bid. Only those agents with access to large amounts of data can effectively compete in this process, creating strong incentives to work with data management platforms who obtain data illicitly or even illegally. If they do not, then the actors who do will likely be more effective in the market.

Cambridge Analytica and **Aggregate IQ** were political consultancies with international operations that became controversial largely as a result of the 2016 UK referendum on European Union membership. One of their functions was as an organisation which accumulated data on individuals and built and applied predictive models to them in order to serve the most easily influenced individuals heavily targeted campaign messages. These messages would be aimed to influence individuals to: i) turn out to vote; ii) remain at home; or iii) to change their mind about their voting preference.

A firm such as Cambridge Analytica and its subcontractors requires data to build a targeting model, and data of individuals to apply that targeting model to. They also need types of identifying information which allow them to target users online. Platforms like Facebook allow email addresses to be uploaded and targeted. On the internet and apps more generally, these companies can act as *data management platforms*, helping advertisers identify and profile visitors to websites with embedded tracking and placing high enough bids on the targeted audience to win the right to show banner ads through *real-time bidding*.

In the United Kingdom, the use of services rendered by Aggregate IQ and Cambridge Analytica was legally contentious for a number of reasons:

- the firm(s) used data obtained through a Facebook plugin created by the University of Cambridge, which scraped data on the friends of those who installed it without their knowledge;
- the firm(s) inferred political opinions of individuals without their explicit consent, which was a violation of the Data Protection Act 1998;

- the firm(s) were unco-operative with the data protection regulators, the Information Commissioner's Office (ICO), refusing to acknowledge its powers or jurisdiction over the data held;
- the activities associated with the firm(s) were funded in a way that was found by the Electoral Commission to breach the law; and
- the firms involved were internationally spread through a complicated corporate structure, such as through affiliated actors in Delaware and Canada, seemingly designed to promote opacity and reduce legal liability.

This case resulted in extensions to the powers of the Information Commissioner's Office and highlighted the need for international co-operation and consideration of jurisdiction in the intersection of data protection and electoral law. Furthermore, the firms raised more general questions about the acceptability of the role of opaque, highly granular profiling and targeting within electoral processes.

Read further: Information Commissioner's Office (2018), *Democracy Disrupted? Personal Information and Political Influence,* ICO.

Box 2.7 Microtargeting and Cambridge Analytica

Attacks on parties and candidates

The Canadian Communications Security Establishment reported '[c]yber threat actors use cyber tools to target the websites, e-mail, social media accounts, and the networks and devices of political parties, candidates, and their staff'.[35] (*Canada's* intelligence agencies also detected six countries attempting to interfere with political party activity in the 2019 general election via in-person activities.[36]) The *United Kingdom's* National Cyber Security Centre has highlighted three types of attacks aimed at political parties in the 2019 European elections,[37] which it states are the three 'most common' in recent years:[38]

1. **Hack and leak** attacks aim to steal sensitive information from parties and/or candidates in order to leak it in an attempt to embarrass or discredit those campaigning.
2. **Hack and post** attacks attempt to gain access to the information dissemination infrastructure of parties to, for example, post misleading or damaging false information to websites, social media accounts or mailing lists.
3. **Insider leaks** are also possible, where motivated insiders share private information from, for example, private messaging groups, in order to create personally advantageous situations within a party.

Parties are increasingly highly selective in targeting voters with specific messages during the campaign and 'get out the vote' efforts on polling day – so a successful attack on the integrity of their voter profiles could also be damaging to those efforts.

Attackers may be attempting to gain access to valuable data assets provided by law, such as electoral rolls (on confidentiality of electoral rolls, see above). Where this is the case, security of political parties is directly connected to the confidentiality of electoral data.

> *'Hacker-for-hire' Andrés 'Sepúlveda's team installed malware in routers in the headquarters of the [Mexican] PRD candidate, which let him tap the phones and computers of anyone using the network, including the candidate. He took similar steps against PAN's Vázquez Mota. When the candidates' teams prepared policy speeches, Sepúlveda had the details as soon as a speechwriter's fingers hit the keyboard. Sepúlveda saw the opponents' upcoming meetings and campaign schedules before their own teams did.*[39]

However, more generally, attacks on political parties can undermine the fairness of the election as a whole, with likely spillover effects on voters' perceptions of the electoral machinery and legitimacy of the outcome as a whole. And many parties (and especially candidates in primaries yet to receive party support[40]) have limited technological capability, outsourcing much of their data processing – even in the *United States*.[41]

Recommendation 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.

2.6 Voting

During an election period, all eligible voters must be able to cast their vote according to the election rules – and ineligible and duplicate votes must be rejected. This means that election officials need mechanisms to check the eligibility of voters to cast a ballot, and to ensure all ballots are included in the final tally. Furthermore, most countries have rules protecting the secrecy of the result until the voting period ends, to prevent early votes influencing later voters.

In this section, we consider the *verification* of the voter and the *casting* of the vote separately, in a cybersecurity context. In the next section, we consider the counting and communications of results. The whole process from voting to results announcement in *South Africa* is shown below in Figure 2.4 (source: Electoral Commission of South Africa).

Figure 2.4 South Africa's voting, counting and results announcement process

Voter verification

During polling, election officials check that an individual is eligible to cast a vote at a specific polling station, before issuing them with a ballot paper or allowing them to use a voting machine. In most countries, this is on the basis of a check against a printed register or 'polling book' (or 'pollbook'), against which valid voters are marked off. In some countries, such as *Pakistan*, these registers also include voter photographs based on other state records, such as national identity documents.[42]

Some jurisdictions (such as in 41 of the *United States of America*, and the District of Columbia), use electronic pollbooks, which can be networked to enable voters to choose a polling place on election day and allow voters to register right up to the election. However, this means the availability of the pollbook system, including any communications links required, is critical to allowing voters to be authenticated. As a backup, EMBs using such systems should ensure a printed list of all eligible voters is sent beforehand to each polling place or that this can be prepared and distributed very quickly. Polling stations in general should have a substantial supply of provisional paper ballots (or equivalent voting machine mechanisms) for those voters that cannot be authenticated in a timely fashion.[43]

Identity document requirements

Not all Commonwealth countries require proof of identity at the polling station. In the *UK (*outside Northern Ireland*)*, identification is not generally required, but ballot papers can later be removed from a count if the eligibility of the voter they are linked to is successfully challenged, since a serial number on ballot paper counterfoils can in such circumstances be used to identify a specific paper.[44] The UK government elected in December 2019 has confirmed plans to introduce a voter ID requirement for elections.[45] *Dominica* is introducing a voter registration card, because the number of registered voters is greater than the population.

In other countries, such as *India, Trinidad and Tobago,* and *South Africa*, a mechanism to prevent duplicate voting is for voters to mark a specific finger or fingernail with an indelible ink that will take several days to disappear, aa shown in Figure 2.5.[46]

Figure 2.5 Indelible ink mark made on a South African voter's thumbnail during the 2009 election

The benefits of requiring voter identification at polling stations are not always clear. One EMB interviewee told us such measures are aimed at improving voters' perceptions of election trustworthiness, rather than actually reducing fraud.

There have been concerns in some countries that minority groups which already under-participate in polls are less likely to possess proof of identity and will therefore be further disadvantaged. In *UK* trials in May 2019, between 0.03 and 0.7 per cent of voters turned away for lack of ID did not return to vote. In two areas, there was a correlation between the proportion of each ward's population with an Asian background and the number of turned-away voters.[47]

Given extremely low levels of impersonation fraud in previous *UK* elections, there were criticisms of the government's plan to mandate the requirement across the country from equality advocates and from the opposition, with one Member of Parliament (MP) claiming the requirements were an attempt 'to suppress voting, and … designed deliberately to hit the poorest hardest'.[48]

In the *United States*, a recent large-scale study concluded voter ID laws 'have no negative effect on registration or turnout, overall, or for any group defined by race, gender, age, or party affiliation', but 'have no effect on fraud either – actual or perceived'.[49] One follow-up study suggested there was some evidence that increased voter mobilisation efforts by the Democratic Party in affected areas counteracted a negative turnout impact of voter ID requirements, although this was rejected as an explanation by the first study.[50]

Biometric authentication

Globally, multiple voting by individuals remains a serious problem for elections.[51] A number of Commonwealth countries, notably *Cameroon, Ghana, Jamaica, Samoa* and *Pakistan*, have used biometric authentication devices to verify the fingerprints or other physiological characteristic of voters at polling stations, registered prior to the election, and to prevent duplicate voter registrations. If connected, these machines can also prevent duplicate voting during polling by individuals – but this brings its own reliability and security risks.

Thirty-five (35) per cent of the respondent Commonwealth countries make use of biometric ID for voter authentication. A breakdown of the proportion of Commonwealth countries (across high-income, middle- and low-income, and small island developing groups) who employ biometric identification, or other identifiers based on government data sources is included in Figure 2.6. The case of *Pakistan* is described in Box 2.8. While such devices can more accurately recognise individuals than election officials, they still have some levels of 'false positives' (where an individual is wrongly accepted) and 'false negatives' (where an individual is wrongly rejected).

A review by Cheeseman et al. concluded 'as a rough rule, biometric registration has tended to work better than biometric verification, simply because the time pressure is so much more intense when millions of voters have to be processed in a single day'. This was apparent in *Chad* in 2016, where the new register apparently eliminated much double registration, but actual voting was still chaotic. In *Kenya's* 2013 elections, a new biometric registration process worked relatively well, producing a register that appeared to have been more transparent than any previous one – although voter identification machinery failed at some point in more than 50 per cent of polling stations.[52] But despite biometric registration, multiple registration still happened in *Somaliland* in 2008 (since the EMB 'did not use the automatic fingerprint recognition software for reasons related to its cost and organizational problems'[53]) and in 700,000 cases in the *Democratic Republic of Congo* in 2011.[54]

Specific biometric technologies can also work less well for some groups – for example, fingerprint recognition often has difficulty with elderly people and manual workers' reduced fingerprints.[55]

During by-elections in September 2017, one Pakistan constituency (NA-120, Lahore) was chosen to test 100 biometric verification machines. These machines do not allow voting themselves, but are designed to assist polling booth staff with the verification task. All voters eligible to vote in this constituency had photographs stored against their identification cards; however, approximately 9 per cent did not have fingerprints stored by the National Database and Registration Authority (NADRA) provided to the Election Commission. Both photograph and fingerprints (where available) were loaded onto these devices, which were procured in 2017 from a Pakistani firm, Secure Tech. Because this was a pilot scheme, these devices were not used to replace normal procedures at the polling booths selected. Instead, voters presented to the machines after placing their vote and were asked to take part in the trial.

In the Pakistani context, there is a lack of evidence in the existence of the specific problem that biometric authentication is designed to solve. In the general elections 2018, where no biometric systems were used, there were no complaints to the Election Commission concerning voter identification issues. Indeed, there used to be a challenge because political pressure meant that it was optional for women to have photographs on voter lists, which would cause problems for the

Election Commission's preferred mode of verification and would have proved an area of controversy concerning allegations of fake votes. This, however, was remedied, and now photographs are obligatory for all on the voter lists. Yet there was considerable wariness of using biometric verification machines with no clear problem identified, particularly following controversies in Kenya and Nigeria concerning these machines.

Read further: Election Commission of Pakistan (2017), *Report of Biometric Verification Machines (BVMs): Pilot Project (NA-120 Lahore-III)*, Election Commission of Pakistan, Islamabad.

Box 2.8 Biometric voter verification trials in Pakistan

In particular, the adoption of biometric identification increases the risk of an attack designed to disrupt elections by misclassifying voters and turning them away. Such incidents might be a result of unintended failures, as well as direct attacks on software (such as through updates or corrupting databases upstream) or hardware or interfaces (such as battery or connectivity failures). And, one study in an African Commonwealth country using biometric voter verification in 2012 found:

> In polling stations with a randomly assigned election observer, [biometric identification] machines were about 50 per cent less likely to experience breakdown as they were in polling stations without observers. We also find that electoral competition in the parliamentary race is strongly associated with machine breakdown. Machine malfunction in turn facilitated election fraud, including overvoting and ballot stuffing, especially where election observers were not present.[56]

Recommendation EMBs using biometric authentication should ensure all eligible voters are easily able to register and vote.

Recommendation 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.

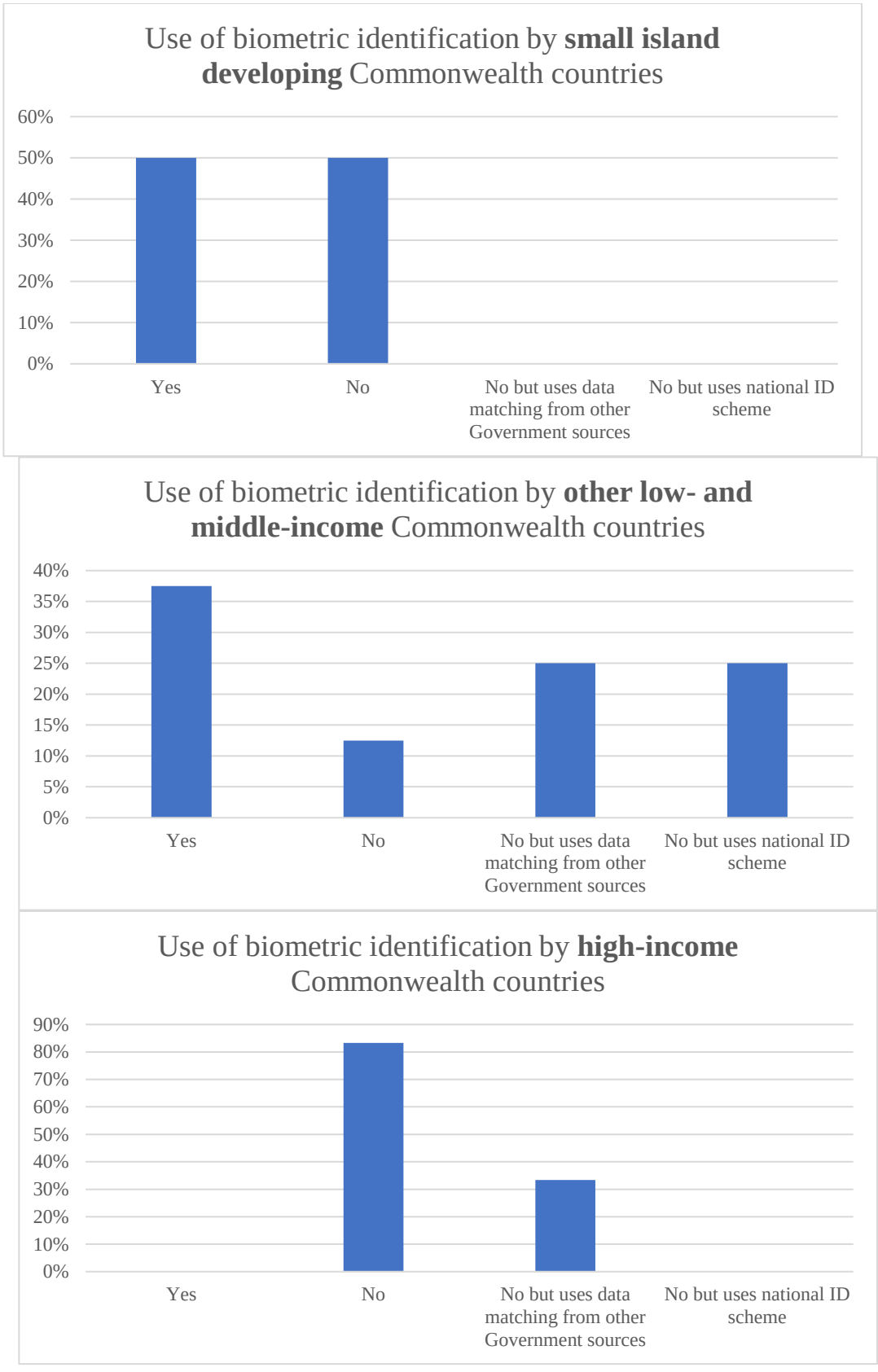


Figure 2.6 Use of biometric identification by respondent EMBs

In 2018, the Malawi Electoral Commission (MEC) introduced the use of a biometric voter registration system to enhance the efficiency of its registration process and to ensure the accuracy of its voter register.

One of the kits used to register voters (comprising a laptop, fingerprint scanner and a camera) went missing in September 2018 and was later retrieved from a train in Mozambique. The media was awash with reports involving missing registration kits, together with cases of duplicate records on the voter register. Rumours circulated on social media that the missing kit had been stolen and was being used to compromise the integrity of Malawi's elections process.

The MEC made various statements and released press releases explaining that nothing sinister had underlined these reports; that the kit had simply been lost in transit and that because of the way in which the kits had been programmed, no-one could gain access to voter data.

The Centre for Multiparty Democracy (CMD) in Malawi, which comprised representatives of all the political parties, commissioned an independent audit of the incident. Digital forensics confirmed that the system at the commission was not compromised in any way and that the data was intact. A copy of the statement issued and signed by members of CMD was circulated to the members so that they could fully appreciate the findings.

The multistakeholder dialogue following the incident proved vital in restoring stakeholder trust in the electoral process. The MEC has since continued to engage certified IT experts to ensure that MEC information technology systems are up to date and not compromised.

Box 2.9 Stolen biometric voter registration kit in Malawi

Vote casting

Most Commonwealth countries – 88 per cent of respondents – require voters to hand mark ballot papers in a physically concealed location in a polling station near their home, or at an embassy or consulate, before placing completed papers in a locked ballot box. Figure 2.6 shows the types of voting seen across country groupings in respondents. Using pencil/pen and paper obviously minimises cybersecurity risks.

Secret ballots reduce the pressure being put on voters to cast their vote for a specific candidate, since they cannot prove afterwards to third parties how they have done so. While over a century old, this mechanism remains critical to fair elections and good governance, since 'multiparty politics in counterfeit democracies often resembles a competitive plutocracy, in which power is wielded by the wealthy' – the rich buy electoral races and governments divert funds to buy votes – 'and poorer citizens rarely secure high political office'.[57]

To protect ballot secrecy, voters are required not to take photographs of their ballot paper – although this has become more of a challenge for election officials given the modern prevalence of smartphone cameras. (Many countries allow some or all voters to cast votes by post or a nominated proxy, particularly those who will be away from polling stations at election time.)

Some Commonwealth countries, notably *India* and *Bangladesh*, use machines in polling stations to record votes from some or all voters. A breakdown of the different types of voting employed across respondent Commonwealth countries is included in Figure 2.1. *India*'s experience with electronic voting machines is described in Box 2.10.

India's electronic voting machines (EMVs) were developed during the 1990s by a state-owned corporation, and introduced into elections from 1998 in an attempt to reduce the incidence of widespread ballot-stuffing (whereby polling stations were taken over by political activists, who inserted false ballot papers into ballot boxes before they were counted). EVMs limited the rate at which votes could be cast to five per minute and featured a 'close' button to disable the device if violence was threatened. The machines also took an impression of voters' thumbprints, which were stored afterwards in an accessible register. Collectively, one study found these measures led to markedly lower numbers of (real plus fake) votes being cast and reduced the vote share of

incumbents, as well as eliminating votes rejected because they were incorrectly marked. Turnout of vulnerable voters increased.[58]

Following concerns about EVM reliability and fraud, in 2011 the Indian Supreme Court ordered the Electoral Commission to consider whether EVMs should produce a voter verifiable paper audit trail (VVPAT) that could be used to check machine counts, ordering in 2013 that these should be introduced.[59] VVPATs were developed and trialled in the 2014 general election, with their use gradually extended to all assembly and general elections. For the 2019 general election, the court ordered that the VVPAT results should be checked against the totals recorded by the EVM for five randomly selected machines per assembly segment, a five-fold increase over the previous Electoral Commission plan of checking 4,125 machine results. The commission estimated this would delay the announcement of results by around four hours.[60]

Box 2.10 The interaction of electronic voting machines and fraud in India

So-called 'direct recording electronic' (DRE) voting machines have been used in a number of jurisdictions around the world. Unlike *India*'s custom-designed machines, many of these systems use specialised software running on general-purpose computers, usually with a Windows or Linux operating system, with some specialised hardware attached.

The *United States* is an example of a country with an extreme diversity of vote casting and counting machines, which are managed by individual counties, as shown in Figure .[61] Recent analysis by *Politico* has shown that of the 596 states (with centralised processes) and counties (with county-run processes) using paperless voting machines tracked, 84 planned to replace them; 82 were in the process of doing so; 35 had completed the switch; 193 had no plans to do so; and 202 did not respond to inquiries.[62]

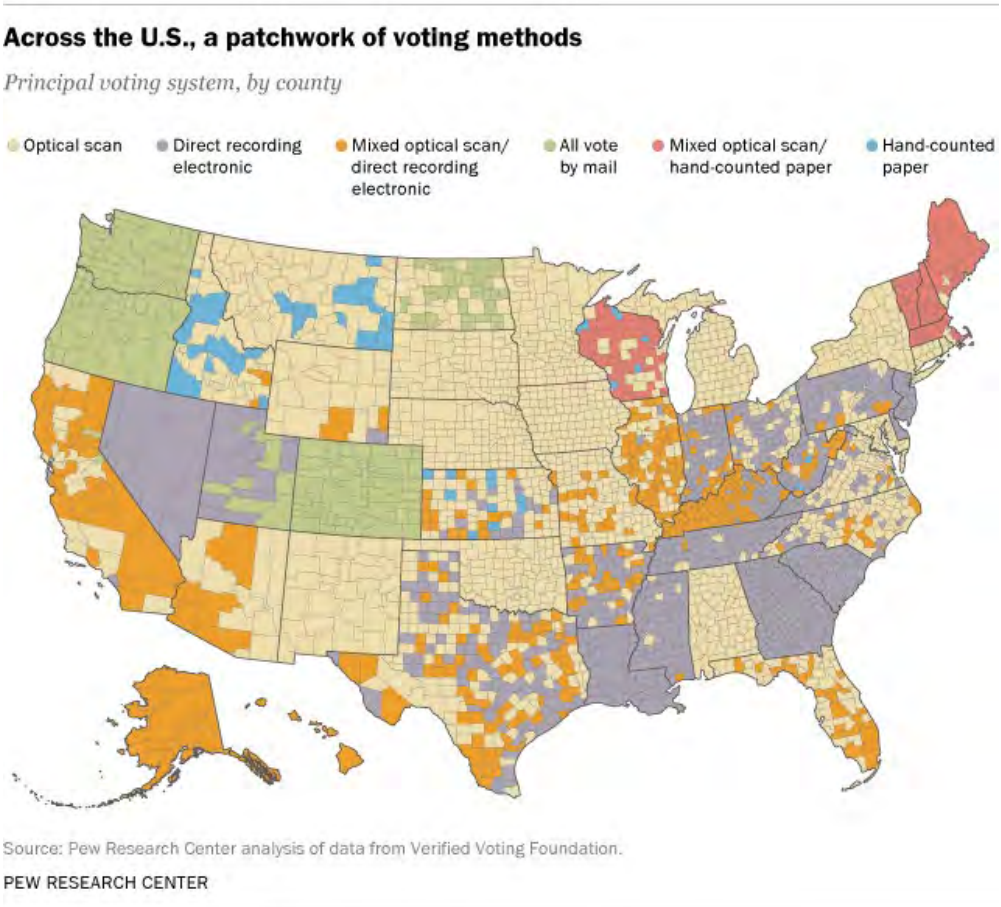


Figure 2.7 USA vote casting and counting systems by county in 2016

DRE systems can instantly tally all votes cast when polls are closed and transmit them electronically to central counting points via mobile data, internet connectivity or other means (such as satellite links in rural areas with limited connectivity). They also eliminate the cost of printing and distributing ballot papers and can provide accessibility support to visually impaired and other voters. However, they can suffer from all of the cybersecurity risks familiar to internet users, even when carefully configured and operated. It also therefore makes them vulnerable to accusations of hacking, even if they are actually secure, potentially impacting voter trust. They are expensive to initially purchase and require ongoing technical support and upgrading.[63]

Polling stations using DREs should have a substantial quantity of paper emergency ballots available, so voting can continue while any faults are remedied.[64]

Voter verified paper audit trails

Because of these potential problems, a number of non-Commonwealth countries have cancelled pilots or moved away from the use of DREs in the last decade, including *Ireland*, the *Netherlands* and *Germany*.[65] The US National Academies of Sciences now recommends: 'All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election'.[66] Retaining **paper ballots** or providing a **voter verified paper audit trail** for voting machines (as required by *India's* Supreme Court in 2013, described in Box 2.10) provides a critical backstop for forensic investigation, court judgments and ultimate public trust in election outcomes.

Even where VVPATS are produced by a machine following an electronically cast vote, the limited research that has taken place so far shows that voters take little notice of them.[67,68] The US National Academies of Sciences concluded that asking voters to hand-mark ballot papers would more likely lead to their vote being recorded accurately.[69]

Germany's Constitutional Court determined in 2009:

> The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject [...] The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections.[70]

Following claims of election hacking in one African Commonwealth country in 2017:

> the limited knowledge of many citizens and commentators regarding how digital processes actually work meant that it was extremely difficult to differentiate false claims from plausible ones. This was revealed in comical fashion when the opposition claimed to have a print-out of the log of activity on the [EMB] servers and distributed it at a press conference only for none of the media, analysts and observers present to have the skills necessary to be able to tell if it was genuine.[71]

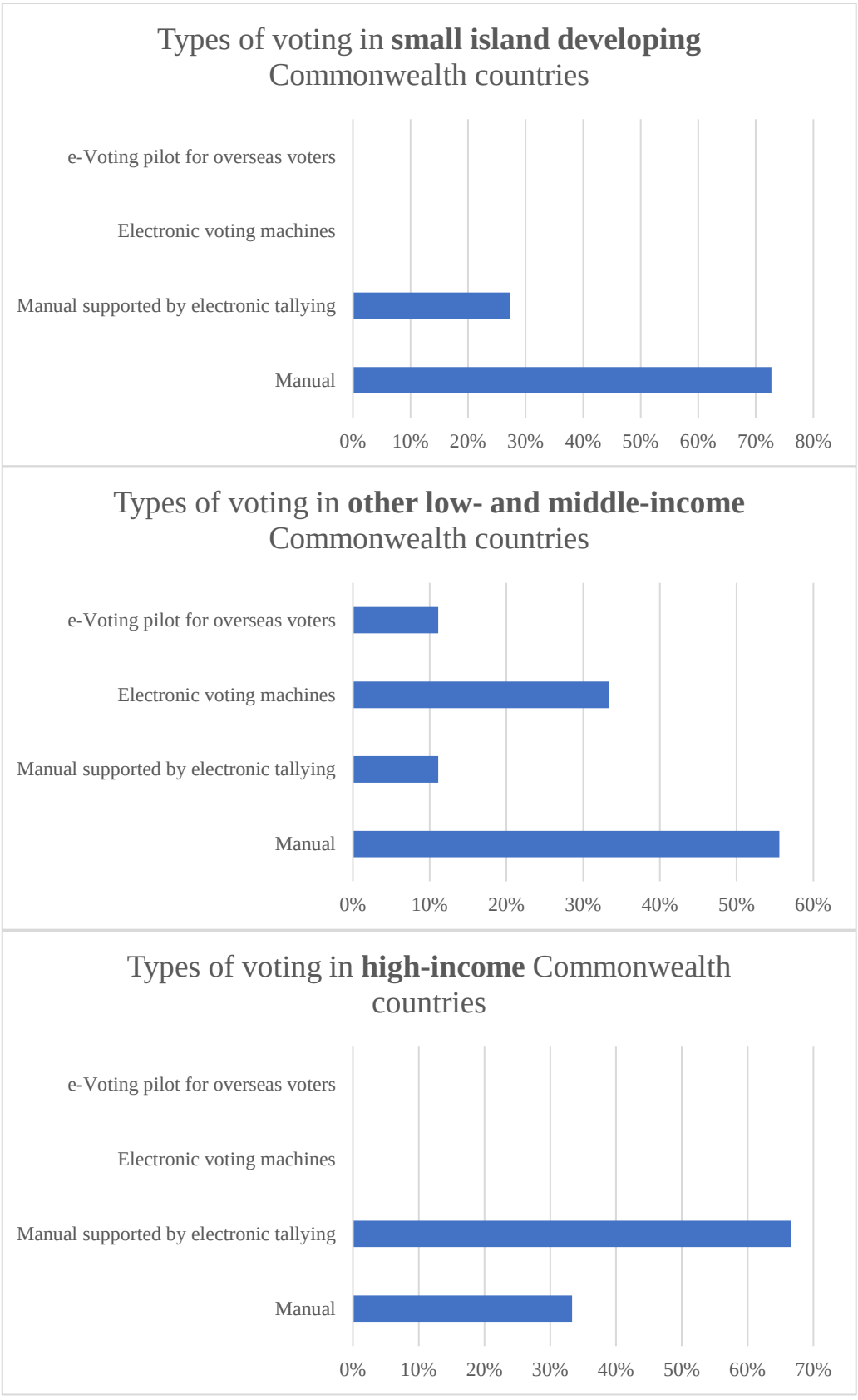


Figure 2.8 Types of voting employed across respondent Commonwealth countries

Recommendation 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.

Accessibility presents an important caveat to general cybersecurity wariness about electronic machines used in vote casting. Some Commonwealth countries allow visually impaired and other specific groups of voters to make use of large print ballot papers and assistive devices to cast their votes. In the *UK*, for example, visually impaired voters can be provided with a Braille-marked tactile device – since these do not include any digital components, they do not raise cybersecurity issues (although note the importance of verifying the correct functionality of the device when acquired).

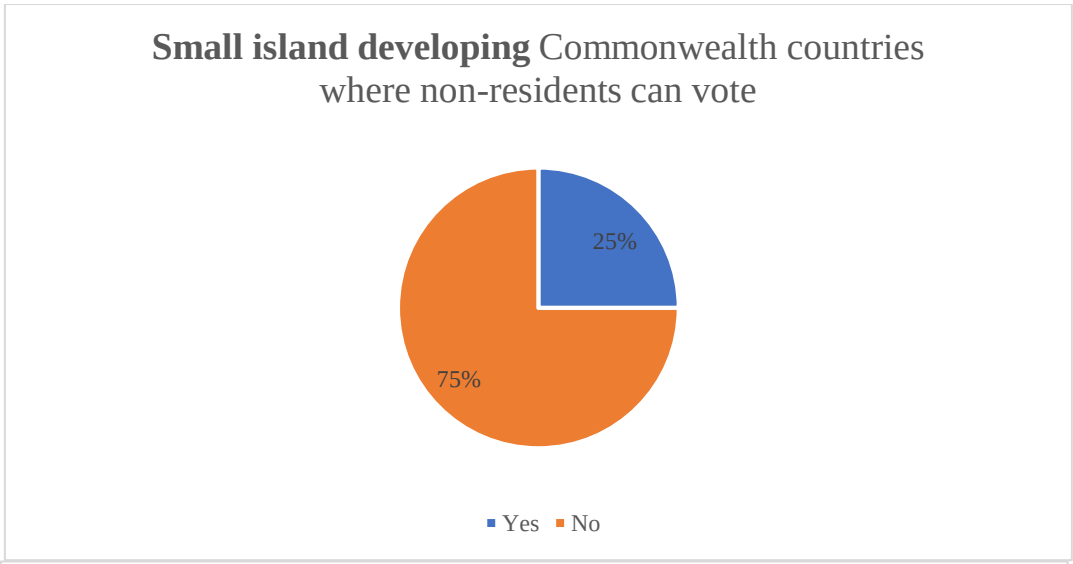
Yet regular surveys by the *UK* Royal National Institute of the Blind (RNIB) have found many of the UK's 350,000 blind and partially sighted voters to be unhappy with the assistive devices provided, with only one in four respondents feeling they were able to vote independently and in secret in the 2017 general election. Only 1 per cent of visually impaired people use Braille.[72] The RNIB is campaigning for the government to 'Provide an online and/or telephone option for blind and partially sighted people to cast their vote independently and in secret if they aren't able to vote at their polling station' in time for the next general election.[73]

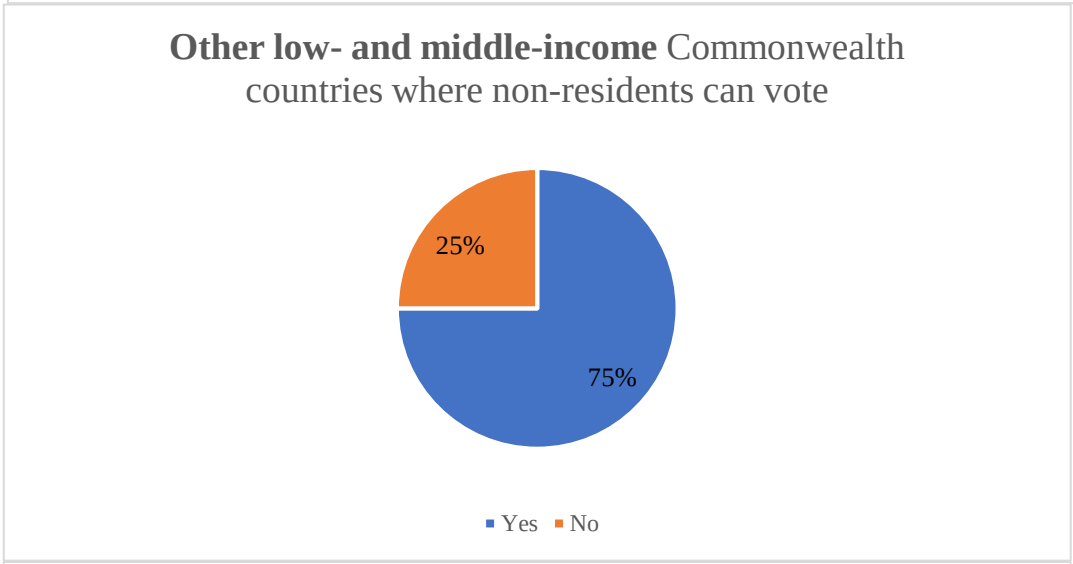
Recommendation EMBs should enable the use of technologies that improve the accessibility of elections for disabled people, while evaluating and carefully managing any resulting cybersecurity risks.

Remote voting

Remote voting has been used in a number of different countries, for reasons ranging from convenience to reaching voters who are conventionally disenfranchised in practice, such as overseas voters. Non-residents can vote in almost half of the respondent Commonwealth countries, though the figure is much lower for small island developing states (see Figure 2.9). Methods for overseas voting that have been deployed by the 115 countries worldwide that, as of 2007, had some remote voting provisions include:[74]

- personal voting, for example, at representations, consulates and embassies;
- postal voting;
- proxy voting;
- voting by fax; and
- internet voting (e-voting or i-voting).





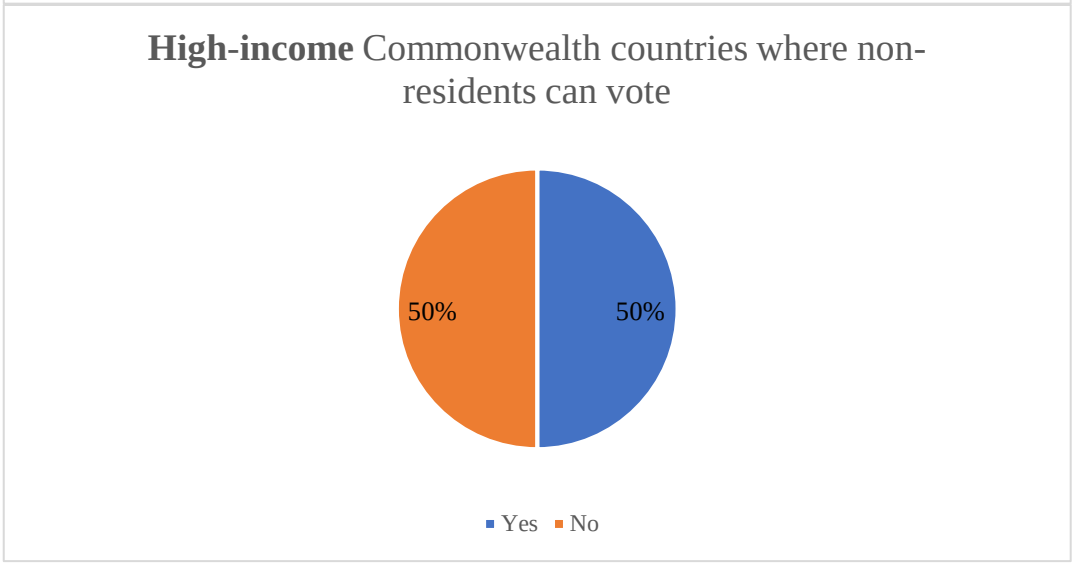


Figure 2.9 Proportion of respondent Commonwealth countries where non-residents can vote

India used a hybrid model for remote voting, which it refers to as an 'electronically transmitted postal ballot system' (ETPBS). This service was first provided to armed forces/services voters and overseas electors, who can register online and also receive ballot papers electronically – which are then printed, completed and physically posted to returning officers. The ballot includes an encrypted QR (Quick-Response) code which can be scanned when the vote is counted.[75]

Box 2.11 India's electronically transmitted postal ballot system

Recommendation 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.

Internet voting

Estonia famously allows votes to be cast from individuals' own computers. Very few other countries have taken this step (*Switzerland* has allowed it for cantonal votes, although Swiss Post recently suspended its system following the identification of security problems by computer scientists,[76] and the *Netherlands* has trialled this method in the past[77]). Estonia is unique in the level of electronic ID, smartcard readers and other infrastructure it already has in place, for the use of a whole range of government services.

Estonian voters can check how their vote has been recorded using their smartphone – reducing although not eliminating the chance it has (accidentally or deliberately) been recorded incorrectly. Voters can also cast multiple votes, with only the final vote being recorded, to reduce the opportunity for voters being pressured into voting in a specific way; 17.6 per cent of eligible voters cast their votes this way in the May 2019 European Parliament elections.[78]

Voter verified paper audit trails generally cannot be produced with internet voting systems. To provide the levels of trust which remotely approach those of paper voting, a highly sophisticated e-ID infrastructure, such as Estonia's, is required, for hardware-grounded trust. Such an e-ID infrastructure would likely rely on an array of cryptographic features to provide assurance, but such approaches are often difficult or impossible to retrofit onto existing ID systems not designed with these types of application in mind.

Many computer security experts have continued to caution against the inherent vulnerabilities introduced by even sophisticated online voting systems. The US National Academies of Sciences concluded in 2018:

> At the present time, the internet (or any network connected to the internet) should not be used for the return of marked ballots. Further, internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the internet.[79]

The topic of the practical arrangement of voting rights for Pakistani citizens has a long history of political discussion. Constitutionally, Pakistani citizens living overseas retain a right to vote, as residency is not a constitutional requirement.[80] In 1993, a petition was filed in the Pakistani Supreme Court where a British-Pakistani law student, Yasmin Khan, sought the right to vote overseas.[81] This petition was heard, and passed to the ministries and the Election Commission to discuss, but ultimately nothing came of it in the subsequent years. Two similar petitions were filed in 2011, calling upon the Supreme Court to issue directions to the Election Commission to prepare electoral rolls for overseas Pakistanis and to take 'appropriate measures for making it possible for the Overseas Pakistanis to cast their vote in Pakistan consulates and embassies'.[82] This led to a request to the Election Commission to undertake such consulate/embassy voting for the 2013 general elections; however, it was not given enough lead time to securely carry this out. The run-up to the 2018 general elections saw the passing of the Elections Act 2017, which addressed the issue in part, permitting the Election Commission to 'conduct pilot projects for voting by Overseas Pakistanis in bye-elections to ascertain the technical efficacy, secrecy, security and financial feasibility of such voting',[83] without specifying the type of voting to be used.

Pakistan had already trialled voting from embassies and consulates and was aware that while this might work for Pakistani expatriates in the United Kingdom where population density allowed

strategic organisation of polling stations abroad, it would be much more challenging in places where diplomatic infrastructure was sparser or populations were more distributed. There were also plans concerning voting by voice – 'tele voting with interactive voice response' – and 'postal ballot using email', which were led by a parliamentary committee in 2015, but these were ultimately not pursued further, in particular following a joint report from the Election Commission and the Ministry of Foreign Affairs about their security and integrity flaws.[84]

Pakistan then considered internet voting or 'i-voting', and there was some pressure to enable overseas voting, in particular i-voting, for the general elections of 2018. However, the Elections Act 2017 only stated that pilot projects 'may' be run and in any case in 'bye-elections'.[85] The Supreme Court determined that the constitutional right of Pakistanis overseas to vote should make these obligatory pilot schemes rather than optional for the Election Commission, and that it should undertake these through its rule-making powers.[86] The pilot schemes need not be restricted to internet voting; there was a mandate for many different approaches to be trialled by the Election Commission. The Election Commission in August 2018 appealed to the Supreme Court to ask that these voting tests be 'pilots' in the sense they had been for the use of biometric verification and voting machines (see below) – that the votes should not count towards any final tally. This was refused by the court.

As a result of this refusal, a series of by-elections that were run in October 2018 *were* undertaken with overseas Pakistanis able to vote through a new 'iVOTE' system. The Electoral Rules were changed in September 2018 to include details of this system, which states that the current policy for voting by overseas Pakistanis is internet voting.[87] Overseas Pakistani voters holding a NICOP identification card, machine readable passport and with an email address, can register with these details, face security questions and be provided with a passcode for voting before polling day. Voting is only open on polling day, as per Pakistani law.[88] The results of these ballots are to be held separately from other votes until the Election Commission is satisfied that the 'technical efficacy, secrecy and security of the voting' has been maintained. At this point, they could be included in the consolidated results.

Internet voting would not be without hazards in Pakistan. Calculated evenly and simplistically, the approximately 6.7 million overseas voters represent just under 20,000 individuals per constituency. In the general elections of 2018, the authors of this report calculate that 32.6 per cent of National Assembly constituencies had a margin of victory of under 10,000; 43 per cent had a margin of under 15,000; and 51.9 per cent had a margin of under 20,000.[89] Individuals are able to vote when abroad in their 'permanent residency' in Pakistan, which is an address (e.g. place of birth) which cannot be changed, unlike their 'temporary address' which may be their place of residence in the country. As a result, it is clear that overseas citizens in Pakistan have considerable political clout. Equally, a controversy of security or integrity of the overseas ballot, when spread across the whole country, comes with the potential to create doubt or distrust in the results of the entire election.

The software used in the i-voting scheme, iVOTE, was an in-house development of the National Database and Registration Authority (NADRA), the agency under the Pakistani Ministry of Interior that regulates government databases, issues and manages the identification system used in Pakistan, and which worked with the Election Commission on the computerised electoral rolls. NADRA has considerable experience and infrastructure for software development and has developed software systems and processes for other Commonwealth countries, such as the Kenyan electronic passport system, the Bangladeshi driver's license system and the Fijian electoral management system, among others.[90]

The Election Commission first discussed i-voting with NADRA. Several types of authentication were considered for voters, including a plug-in biometric device, given the fingerprint data and collection infrastructure NADRA manages regarding Pakistani citizens, or authentication based on webcam data, given that images of individuals are the main mode of verification at ballot stations in Pakistan today. These ideas were not received well in parliament given their complexity, and particularly considering that many Pakistanis abroad do not have webcams or laptops into which they can plug peripherals. A large number of Pakistanis abroad are based in the Middle East and in Gulf states, and literacy levels are low in some professions.

NADRA's proposed solution to this was to use the numbers on machine-readable passports as a verification method in co-ordination with a NICOP number. This was known as the remote identity proofing (RIDP) system.[91] The iVOTE system subsequently developed (in Java) was tested for three months in-house by NADRA's lead penetration tester as a first approach to analysing its security. The iVOTE system was demonstrated to the Supreme Court on 12 April 2018, in a session including a variety of political parties, computing academics from Pakistani universities, citizens and media outlets.[92]

This was followed by an external task force, the Internet Voting Task Force (IVTF), which was established by an order of the Election Commission, 'mandated to assess the overall web-based automated system of internet voting for eligible Pakistani voters living abroad'.[93] This task force was to audit and evaluate the system for various vulnerabilities. The task force included primarily academics and a Dubai-based firm, IT-Butler, run by a Pakistani national that the Election Commission also used for training and the seeking of international cybersecurity standards and certification. The IVTF Report that resulted from this study, which is publicly available, highlighted a range of concerns, including the following:

- iVOTE did not provide the ballot secrecy required in the Constitution of Pakistan and in the Elections Act 2017.[94] This was inherent to the computational approach taken in iVOTE, rather than a failing of the software implementation.
- Voter coercion and vote buying were very possible in this system.
- A particular vulnerability was allowing users to choose their constituency within the voting system outside of that which they are registered.
- The website and interface were vulnerable to being impersonated in phishing attacks.
- The DDoS-protection utilised by NADRA could compromise ballot secrecy, exacerbated by the foreign nature of the external provider.
- iVOTE employed deprecated and compromised third-party components.
- No usability studies had been carried out, particularly in relation to low-literacy individuals, which in turn might raise new security concerns.
- iVOTE emails could be blocked by spam filters.
- iVOTE did not offer the verification or redundancy features in other jurisdictions with experience in internet voting.
- There was no threat model analysis or code documentation.
- There was no known resource planning for monitoring iVOTE on polling day.
- There was no known planning for preventing insider attacks.
- Newer technologies and architectures should be considered.

This public report did not contain specific details of these vulnerabilities. NADRA fixed the specific vulnerabilities described by the task force, and the lengthier report with the vulnerabilities in is subject to a non-disclosure agreement between the Elections Commission and NADRA and is kept securely in the Elections Commission, outside of normal data systems. The public report contains a breakdown of vulnerabilities by type and severity and presents broader recommendations.

Following this report, which was then presented to the Supreme Court and to the ECP in May 2018, the Supreme Court ruled that such a system should go ahead and be trialled in the impending by-elections in October 2018. These by-elections represented 35 constituencies, which were electing 11 National Assembly seats and 26 Provincial Assembly seats. Some 639,909 overseas Pakistanis would have been eligible to vote for these by-elections, of which in the relatively short 17 days available for registration, 7,419 registered (351 of which were later excluded due to their constituencies running unopposed). Video tutorials on how to use the system were provided in English and Urdu.[95] Of those remaining, 6,223 exercised their voting rights on polling day itself: an 83.54 per cent turnout rate. The Election Commission was aware few registered, but the cause of this was unclear. In particular, it was unclear whether there was little demand from outside the country (compared to the considerable political appetite for overseas voting from some actors within the country); whether by-elections were not interesting or salient enough democratic events; or whether there was limited awareness of the iVOTE system. In the end, following reflection on the process, the Election Commission did not exercise its powers to ignore these votes for reasons of technical efficacy, secrecy or security, and instead included the votes into the final counts.

Polling day itself did see some minor DDoS attacks, ostensibly primarily from Russian IP addresses: these were successfully defended against and did not present issues. There were no reports of abnormalities relating to registration or phishing, and the high turnout of the vote attested to the availability of the service to at least accounts that had pre-registered.

The report of the scheme[96] was laid before parliament on 14 January 2019. At the time of writing, Pakistan was waiting to see if parliament would agree to internet voting in future elections, particularly given the implications for ballot secrecy, which is particularly sensitive given the risk posed by those in coercive positions, such as heads of households or ringleaders or co-ordinators of

labourers, gathering votes and using them collectively. Whether the iVOTE scheme is expanded to a general election was at the time of writing in the hands of parliamentarians and would require an amendment of the Elections Act 2017 to expressly permit.

Box 2.12 Internet voting trials in Pakistan

Recommendation 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.

Vote counting

In most Commonwealth countries, election officials count ballot papers by hand at either polling stations (e.g. *Pakistan* and *Trinidad and Tobago*) or constituency or regional counting centres (e.g. *Ghana* and the *UK*). In most countries, party agents are permitted to observe the count and in some (such as *Pakistan* and *Trinidad and Tobago*) are asked to sign the forms used by officials to record the accepted results.

Where results are extremely close, candidates may commonly request recounts. This is important for accuracy, given that hand counting is an extremely repetitive process where small mistakes can easily be made, even while maximising the transparency of the process.

In some Commonwealth countries, such as *Australia* and *Malta*, optical scanners are used to rapidly count votes marked on ballot papers.[97] This can particularly increase the speed of counting where proportional voting systems are used, and voters can specify preferences between a number of candidates.

In *Kyrgyzstan*, voters place hand-marked ballots into a scanner which reads the vote, then deposits accepted papers into the main 'bin', diverting rejected ballots into a special 'bin'. When voting closes, the scanners are connected to the internet, displaying the results and sending them to the Central Election Commission (CEC). A hand count is performed and the ballots in the rejected bin are added to the main count if their intention is clear. The results of the hand count are sent to the CEC when complete and, in case of discrepancy, the hand count takes precedence.[98]

In the *UK*, many returning officers use digital systems to help verify the voter information and signature on the outside of an inner envelope containing postal ballots, before valid ballots are delivered to the relevant counting centre to be included after the close of polling. Lack of public understanding of this system – despite extremely clear public information from the Electoral Commission – led to thousands of tweets following the December 2019 general election questioning why a company with a board member linked to one party had been counting postal ballots (it had not).[99] There were also public (unproven) claims about voting patterns on postal ballots before polling day, repeated to great controversy by the BBC's political editor one week before the election.[100]

Recommendation Systems to verify postal ballots should be carefully designed to maintain public trust and the confidentiality of votes.

In all cases, mechanisms are needed both for consideration of ballot papers where marks are unclear – often requiring a consensus of observing party agents – and for verifying counts, especially where they are close. This can be done by checking results against a hand count of a statistically significant sample of ballot papers.

South Africa conducts an external audit of results, with every results slip compared with the captured version. In addition, every results slip is scanned and made available to political parties for verification. Political parties witness counting and sign the completed results slips at every voting station.

Recommendation EMB officials should examine and determine how to treat every ballot rejected by automatic counting systems as invalid or uncertain.

Risk-limiting audits

The concept of 'risk-limiting audits' has emerged as a best practice in EMB approaches to efficient results auditing, where machines are used to cast and/or count ballots.[101] Before the result is certified, a fraction of such ballot papers are selected for hand counting, to compare against the machine totals. The sample size (percentage of randomly selected ballot papers) is increased as the margin of victory for the winning candidate or party decreases, ensuring the optically scanned and hand-counted results match to within an agreed statistical margin of error. Basic additional checks can also be carried out, such as ensuring the number of votes cast corresponds to the same number of votes marked off in poll books.

Recommendation Where ballot papers are scanned and counted electronically, EMBs should run risk-limiting audits to check results to build public confidence in election results.

2.7 Communication of results

Digital communication of results by election officials once they are counted – preliminary and final – presents significant opportunities for attacks on electoral integrity, but also opportunities to make information (such as photos of preliminary results sheets) more widely available and hence effective as a tool for third parties to detect fraud. 'Parallel vote tabulations' are often undertaken by political parties, the media and electoral observers, and are an important tool for improving the reliability of results reporting.[102]

Reporting that is incorrect – from cybersecurity failures upstream or integrity attacks on the communication process – presents a clear threat to the perceived integrity of the democratic process, even if speedily rectified. Availability attacks on communications infrastructures or standard operating procedures for delivering results can foster suspicion and tension, which might even erupt violently or trigger other consequences with detrimental impacts. Without timely control of reporting, results are open to opportunistic pre-emption, meaning the EMB can lose control of information dissemination, framing and the overall electoral narrative.

Transmission

In some Commonwealth countries where responsibilities are devolved to local jurisdictions and the electoral system does not require cross-constituency calculations (often needed in proportional voting systems), results for each local constituency can simply be announced by election officials at the counting centre (see, for example, the *United Kingdom*) and reported directly to parliamentary authorities. Such mechanisms do not require the use of transmission or tabulation systems (aggregation in news reporting is done by the media). Election data can eventually be released on the EMB website and archived as national law dictates. Such decentralised systems can be considered more secure than those which are centralised, as they do not have one single point of failure, although they may bring risks of difficult-to-spot counting failure or unwarranted data retention, and have fewer cybersecurity resources available than a central authority.

In more centralised electoral systems, the organisation which counts votes will also be responsible for dissemination. *Australia*'s Electoral Commission carries out such a role via its website and Twitter feed, from which media organisations and social media can receive updates during the 18-hour House of Representatives and multi-day Senate voting process. Some countries show a degree of centralisation in the communication of results, as there may be a need for aggregation and transmission first on a regional level before results are communicated centrally.

In **Ghana** vote counting and collation is done manually. Results are collated by district, constituency and then finally nationally at the Electoral Commission of Ghana's (ECG) headquarters. Returning officers use fax initially. The ECG waits until the manual process of checking, collating and delivery is completed before announcing the certified results. This process can often take up to 72 hours, to allow delivery from remote areas that are not easily accessible. As polling stations and collation centres are required to display results once they have tallied votes, parallel systems for the collation and transmission of votes have been set up by both parties and the media. While some interviewees noted that this transparency measure proves vital for preserving trust in the elections process, it

often means there is a large gap in the reporting of the provisional and certified results – and this leads to public frustration and periods of political instability. Consequently, the ECG is trialling new forms of transmission in order to speed the process up.[103]

Box 2.13 Vote counting and collation in Ghana

Centralised election systems will often require the EMB to **administer transmission channels** in order to retrieve local counts, to **input data to tabulation systems** and to **calculate the final result**. Transmission channels can include the following:

- Manual delivery of counts by hand: These can be vulnerable to physical interception, modification and theft, without physical security measures such as police escorts.
- Telephone, fax and satellite: Earlier generations of telecommunications systems did not include security protections for transmitted information.
- Uploads to dedicated software via direct connections: For example, virtual private networks (VPNs) or the internet, which will usually include end-to-end encryption protection for the confidentiality and integrity of transmitted information.
- So-called 'over-the-top' communication services such as WhatsApp and Signal: These add end-to-end protection to transmitted messages.
- Direct or indirect connections to e-voting devices: To reduce the risk of compromise, such devices should be isolated from public networks. But even if USB sticks or similar plug-in memory sticks are used to download results from devices, this does not eliminate the risk of malicious software on such removable media attacking devices when they are plugged in.

As with all the other aspects of the electoral cycle, connection to networks that involve the transfer of data from one component to another will pose risks of manipulation. EMBs should arrange parallel systems of transmission, where possible relying on distinct networks, software and hardware, to mitigate against integrity and availability compromises. *India,* for example, conducts dry runs prior to an election and has 200 per cent server redundancy (the duplication of critical components or functions of a system usually in the form of a backup or a fail-safe) in the event that the main network malfunctions or there is a power failure. In all cases, final certification of results should make use of original paper results forms from polling stations and counting centres, which are amenable to forensic analysis. Original ballots and results forms should be securely preserved as evidence in any future challenge to results.

Without enough time for testing, one African Commonwealth country found in a 2013 election '[e]arly result transmissions recorded a remarkably high number of rejected ballots; it was then announced that the system had arbitrarily multiplied the number of rejected ballots by eight, though how and why has never been explained. Then, following an initial stream of results, the flow of information ground to a halt'.[104] And in *Azerbaijan's* 2013 election, 'the credibility of a mobile phone app purportedly designed to communicate results was fatally undermined when it released the figures a day before a single ballot had been cast'.[105]

Recommendation 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. Final results certification should depend on verification of original signed count forms.

Recommendation 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.

Tabulation and aggregation

Tabulation systems will be required to aggregate votes in cases where vote counts are centrally located. This will often involve the use of dedicated software to tally transmitted vote data. Such software must be properly audited and tested before use. Any changes should

be carefully documented and subject to version control, and sufficient training must be provided to users of the chosen tools.

Approaches using common and easily changed software, such as spreadsheets containing automatic formulae, are prone to alteration. Public sector best practice in maintaining software such as this should be followed. Following a scandal involving incorrect spreadsheet formulae in a procurement process, the *UK* created processes for providing quality assurance to high-risk spreadsheet-based tools in its 'Aqua Book', many elements of which will apply even to simple and predictable tabulation approaches.[106]

As a large country with a constitutional requirement to hold elections in a single day, as well as a history of disrupted democracy, in **Pakistan** the system for transmitting results in a reliable form emerged as an important political concern. The Elections Act 2017 in Pakistan introduced a new, photographic mechanism for results transmission. Presiding officers have been trained to use a smartphone app to photograph 'Form 45' – the document which was manually taken from polling stations to a central centre under the pre-existing system. In the 2018 Pakistani general elections, 51 per cent of results were sent through the new system. In some areas, the installation of satellite internet was required. On polling day, an attempted denial of service attack on the transmission system was thwarted.[107]

Box 2.14 Results transmission in Pakistan

Tabulation is an easy point in the electoral process for errors to occur, and the ease of errors can be exploited by malicious actors wishing to undermine electoral integrity.

Recommendation EMBs should ensure software used in vote tabulation is audited and verified, and used by trained staff on appropriately secured hardware.

Publication

Publication and documentation of official results via the election portal on EMBs' websites in a timely manner is important to many EMBs and voters alike. *South Africa's* EMB provides a live results feed to the media, on screens, and via an application programming interface (API) which allows third parties to include the results in their own tools. Results operations centres (ROCs) are in operation in each of the nine provinces and at the national level from election day until results are announced, which enables the EMB, political parties and the media to operate from the same venues and have regular meetings and/or press briefings. The Parliamentary Election Office of *Grenada* has installed a server to enable the media to access official election results.

Further information can also be provided to increase election transparency – for example, *Malawi*'s EMB publishes images of all results sheets on its website, enabling third parties to check for any signs of fraud and promoting public confidence in results.[108]

Attackers can conduct denial of service attacks on a results portal, just as they can for any public facing website, making reporting unavailable and thereby undermining voter confidence. The data is also subject to manipulation if attackers gain unauthorised access. Another possibility is that voters are redirected to spoof websites which purport to demonstrate official results.

In one African Commonwealth country 2017 election, 'results quickly began to flow into the online system, which was connected to a new – and impressive – website that allowed citizens to search results to the polling station level. However, as more information about the election began to trickle out, it transpired that some parts of the system had not been strengthened. Most notably, around a quarter of the scanned forms were not transmitted and made available by the time that the election result was announced. It also transpired that the passwords of senior

election officials were used to access the system thousands of times – potentially by different people'.[109]

Although in all Commonwealth countries there are multiple sources of media reporting and therefore no one single point of failure, broadcasters and online news outlets still pose a vulnerability – particularly if a sophisticated actor had the means to conduct simultaneous attacks on multiple outlets. Even if the correct results can be broadcast effectively in time, there is a risk of immediate disruption or violence. In one example of a narrowly avoided incident, Russian-speaking hackers compromised the website of *Ukraine*'s Central Election Commission, changing the result, which was noticed and corrected by officials just one hour before it was due to be announced. Despite this, the fake result was broadcast by Russian state media.[110]

While it may seem attractive to deliver results using new tools, such as specifically developed apps, or over new social media channels, these present emerging risks. Figure 2.10 shows the use (and frequency) of social media types across EMBs for the communication of results and other purposes. EMBs should disseminate results online only in forums they are confident they have the expertise and resource to adequately secure. At the time of writing, this will likely be their own websites, and large-scale web hosting and social media services. Even then, during the *UK*'s 2016 referendum on leaving the European Union, a last-minute online registration surge led to the Electoral Commission's registration website crashing. Fortunately, parliament was still sitting and able to extend the registration deadline – which would not have been the case before an election, as parliament is dissolved 25 working days before polling day.

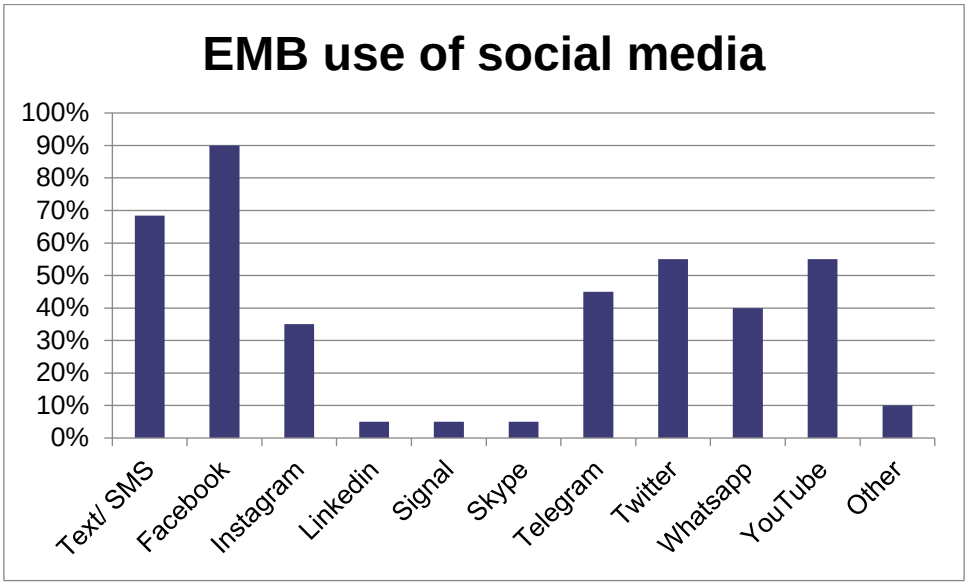


Figure 2.10 Respondent EMB use of social media

Recommendation EMB websites, especially those announcing election results, should be protected against high levels of traffic and denial of service attacks.

The Election Commission of **India** results website recorded 812.3 million hits in one single day during its recent elections. To address its security, the commission undertook major training starting from end users to the application. Various government agencies looking after cybersecurity were put on high alert, traffic on the network was regularly monitored and various cybersecurity layers were put into place to ensure the integrity and availability of the elections system. The commission had support against denial of service attacks from CloudFlare and used features in the database software MongoDB to support the storage of 910 million voter records.

The commission also displayed the real-time results of the election on its mobile app, allowing users to see the authentic results directly from their phone, anywhere. The user could view these results by scanning the barcode of their commission-issued voter-ID. The Election Commission had designed

this innovative mobile application, which was called the Voter Helpline. This mobile application connected five databases together and prepared seamless services for citizens; it allowed searching of their names from the 910 million in a fraction of a second. The voter could verify their name, the polling station, details on the voter card and also the election schedule. If they already had a voter ID card, simply by calling the voter ID card the details can be verified.

Box 2.15 Results reporting in India

It is of course open to electoral authorities acting unlawfully to simply announce results that do not correspond to the votes cast. In the August 2017 vote in *Venezuela* for a new constituent assembly, the Electoral Council announced that 8.1 million people – 41.5 per cent of the electorate – had voted in favour of the new assembly. But the CEO of the company Smartmatic, which provided the voting machines used, reported this figure had been inflated by at least one million voters.[111] *Reuters* reported an internal memo from the council stating only 3.7 million votes had been cast two hours before polls closed. The country's chief prosecutor stated: 'I'm absolutely sure that those numbers are not correct'.[112] In a second example from the 2018 presidential elections in *Democratic Republic of Congo*, analysis by the *Financial Times* of tallies from 62,716 voting machines obtained from the Electoral Commission's central database, as well as a parallel vote tabulation conducted by 40,000 observers from the Catholic Church, demonstrated the second-placed candidate had been wrongly announced as the winner.[113]

Both cases demonstrate that careful analysis of the large volumes of data produced by voter authentication and casting systems can be used to detect electoral fraud. A Congolese Electoral Commission whistle-blower, 'imprisoned and tortured for nine days in the DRC' in 2017, has since been given refugee status in the UK.[114]

2.8 Auditing and challenging results

The ability to verify accurate results is a strict requirement of any free and fair election. Many actors are involved in auditing: the EMB is responsible for documenting evidence and auditing all aspects of its processes as a matter of course; national courts in the event of a legal challenge to the validity of a result; and national parliaments and political organisations, civil society groups and external election observers (including, for example, Commonwealth Observer Groups), provide additional layers of accountability. If these processes demonstrate that an election result cannot be deemed a valid democratic outcome, then a key backstop in any election is the provision for recounts, should they be required.

As the dependence of all elections on digital technologies grows, so do challenges to the audit process. If IT infrastructure is compromised at any stage of the electoral cycle, then the reliability of the information used to determine the outcome can be questioned. This makes the reliable recording and storage of data critical and emphasises both the usefulness of authoritative paper ballots and forms, and the publication of intermediate and final results.

Archiving of systems, processes and outcomes is crucial, but electronic archives in particular might also be subject to attack, particularly with an aim to destroy or tamper with them. While EMBs commonly have data retention systems in place for the safekeeping of physical or paper resources used throughout the electoral cycle,[115] systems for storing and safeguarding electronic data are likely newer and may not be as complete as desirable for such audits. Important data to audit might include:

- 'snapshots' of the versions of any critical software or firmware deployed during the election on, for example, voting machines, biometric verification machines or tabulation systems;
- copies of relevant e-polling books, in accordance with laws on retention governing electoral rolls;
- appropriately granular voting data, well organised alongside metadata and clearly documented;
- instructive documentation, including online documentation and guidance, provided to staff and volunteers; and
- web logs from critical systems.

In countries which require elections processes to be transparent, this information may be opened up to external observers and even citizens. Secure facilities, processes and training for non-EMB staff to access and check this data may need to be considered. And pre-election training of the judiciary in election technologies and cybersecurity mechanisms that are in place will facilitate any legal challenges brought following an election, as *Malawi* has found.

Rather than aiding transparency, the extremely high level of IT knowledge and expertise required to understand how integrated electoral management systems work, and what is implied about the process if they do not, means that opposition parties and international monitors are often poorly placed to evaluate the quality of the process – even in relatively technologically savvy states.[116]

The Electoral Commission of South Africa enables a broad range of independent audits to be undertaken of South African elections, to build public confidence in the outcomes. These include:

- independent audit of the results systems;
- independent ICT network security audit focusing on network vulnerability, penetration testing, systems access controls and data protection – both external and internal threads;
- independent network security assessment and/or audit by the State Security Agency; and
- political parties as key stakeholders being invited to independently audit the results system, to assure themselves that the system works as intended and prescribed in law;

Box 2.16 Independent audits of South African elections

Source: South Africa Electoral Commission

A common misperception is that the release of information about system security can reduce that security and that transparency can create new vulnerabilities. One can assume that any adversary should know these details already and that transparency can instead help security researchers identify and remedy cybersecurity gaps.[117] The more salient threat to the election process is that the auditing process itself can be manipulated, in order to introduce doubts about the validity of the process, thereby prompting electoral disputes and potentially costly reruns.

Recommendation 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.

Notes and references

[1] Canada Communications Security Establishment (2019), *2019 Update: Cyber Threats to Canada's Democratic Process*, February, p.17

[2] See, for example, the Cambridge Analytica scandal, centred in part on datasets collected illegally using Facebook: Information Commissioner's Office (2018), 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', 25 October, ICO (Cheshire, United Kingdom). See also the fine to the parenting club 'Bounty' for providing data to the UK Labour Party: Information Commissioner's Office (2019), 'Bounty UK fined £400,000 for sharing personal data unlawfully', 12 April, ICO (Cheshire, United Kingdom).

[3] See Electoral Commission (2018), 'Vote Leave fined and referred to the police for breaking electoral law', 17 July, Electoral Commission [UK].

[4] International Institute for Democracy and Electoral Assistance (IDEA) (2015), 'Certification of ICTs in Elections', December, p.13, available at: https://www.idea.int/publications/catalogue/certification-icts-elections.

[5] Ellen Nakashima and Shane Harris (2018), 'How the Russians hacked the DNC and passed its emails to WikiLeaks', *The Washington Post*, 13 July, available at: https://www.washingtonpost.com/world/national-

security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html
[6] Matthew Cole, Richard Esposito, Sam Biddle and Ryan Grum (2017), 'Top-Secret NSA Report Details Hacking Effort Days Before 2016 Election', *The Intercept*, 5 June, available at: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/
[7] Seda Gürses and Joris van Hoboken (2018), 'Privacy after the Agile Turn', in Evan Selinger and others (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press.
[8] EU Foreign Affairs Council (2018), Council conclusions on malicious cyber activities, 16 April, Brussels, p.2, available at: http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf
[9] See, generally, Vasilios Mavroudis and others (2017), 'A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components', in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (CCS '17), ACM, New York, NY.
[10] Edgardo Cortés, Gowri Ramachandran, Liz Howard and Lawrence Norden (2019), *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials*, Brennan Center for Justice, p.8, available at: https://www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf
[11] *McEwing and Kerr v Canada (Attorney General)* [2013] FC 525.
[12] *R v Sona* [2014] ONCA 859; see, generally, Michael Pal (2017), 'Canadian Election Administration on Trial: "Robocalls", Opitz and Disputed Elections in the Courts', 28 *King's Law Journal* 324.
[13] Michael Pal (2017), op. cit. endnote 1.
[14] *WM Morrison Supermarkets Plc ('Morrisons') v Various Claimants* [2018] EWCA Civ 2339.
[15] Canada Communications Security Establishment (2019), p.16, op. cit. endnote 1.
[16] In 2018, for example, the Knox County Tennessee election night results reporting website was taken temporarily offline following a DDoS attack. No votes were tampered with, but the attack successfully caused concerns that the election had been compromised and that a larger attack was underway. See Center for Democracy and Technology (2018), *Election Cybersecurity 101 Field Guide – DDoS Attack Mitigation*, November, available at: https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/
[17] Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization* 25(8), p.1398.

[19] See, for example, Center for Internet Security (2018), *A Handbook for Elections Infrastructure Security*, February, p.15.
[20] The Representation of the People (England and Wales) (Amendment) Regulations 2002, reg 106. See, generally, the Electoral Commission (2019), *Guidance for Electoral Registration Officers,* 'Part 4 – Maintaining the register throughout the year', Electoral Commission [UK].
[21] Commonwealth Electoral Act [Australia] 1918.
[22] Canada Elections Act (SC 2000, c. 9) s 101.
[23] Election Act [Pakistan] 2017 s 79(3).
[24] Such provisions may be provided for in overarching privacy and data protection law, in electoral law, or, in some cases, these data may be re-used by political parties and fall out of legal safeguards.
[25] Jason Murdock (2016), 'Mexico election hack: Political party behind leak of 93.4 million voter records?', *International Business Times*, 25 April, available at: https://www.ibtimes.co.uk/mexico-election-hack-political-party-behind-leak-93-4-million-voter-records-1556608
[26] 'Hackeo masivo al padrón del INE', *El Universal*, 13 September 2017, available at: https://www.eluniversal.com.mx/nacion/politica/hackeo-masivo-al-padron-del-ine
[27] Melissa Galván (2018), 'El INE denuncia la venta en internet de una copia de la lista de electores', *EXPANSIÓN politica*, 7 October, available at: https://politica.expansion.mx/mexico/2018/10/07/el-ine-denuncia-la-venta-en-internet-de-una-copia-de-la-lista-de-electores
[28] Ibid.
[29] UK Electoral Commission (2019), 'Modernising electoral registration: feasibility studies', available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/a-modern-electoral-register/modernising-electoral-registration-feasibility-studies
[30] Centre of Excellence for CRVS Systems and the Global Partnership for Sustainable Development Data (2019), *A Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, International Development Research Centre, p.118, available at: https://www.idrc.ca/en/news/compendium-good-practices-linking-civil-registration-and-vital-statistics-and-identity
[31] American Civil Liberties Union (ACLU) (2018), 'Federal Court Blocks Indiana Voter Purge Crosscheck Law', ACLU, https://www.aclu.org/press-releases/federal-court-blocks-indiana-voter-purge-crosscheck-law (accessed 7 July 2019).
[32] Nic Cheeseman and Brian Klaas (2019), *How to Rig an Election*, Yale University Press, New Haven, p.47.
[33] UK Government, 'Register to Vote', available at: https://www.gov.uk/register-to-vote (accessed 4 November 2019).

[34] See, generally, Information Commissioner's Office (2019), 'Update Report into Adtech and Real Time Bidding', 20 June.
[35] Canada Communications Security Establishment (2019), op. cit., p.5
[36] Catharine Tunney and Ashley Burke (2019), 'Federal parties being warned of efforts by 6 foreign countries to influence election: sources', CBC News, 16 September, available at: https://www.cbc.ca/news/politics/china-india-interference-1.5284473
[37] National Cyber Security Centre (NCSC) (2019), Guidance for political parties, NCSC [UK], available at: https://www.ncsc.gov.uk/guidance/guidance-for-political-parties
[38] National Cyber Security Centre (2019), Guidance for individuals in politics, NCSC [UK], available at: https://www.ncsc.gov.uk/guidance/guidance-for-individuals-in-politics
[39] Jordan Robertson, Michael Riley and Andrew Willis (2016), 'How to Hack an Election', *Bloomberg Businessweek*, 31 March, available at: https://www.bloomberg.com/features/2016-how-to-hack-an-election/
[40] Maciej Cegłowski (2019), 'What I Learned Trying To Secure Congressional Campaigns', *Idle Words*, 26 May, available at: https://idlewords.com/2019/05/what_i_learned_trying_to_secure_congressional_campaigns.htm
[41] Alyza Sebenius and Kartikay Mehrotra (2020), 'Iowa Caucus Results Saved by Plain Old Paper After App Fails', Bloomberg News, 4 February, available at: https://www.bloomberg.com/news/articles/2020-02-04/iowa-caucus-results-saved-by-plain-old-paper-after-app-fails
[42] However, research shows people are bad at matching individuals to photos. See, generally, Ross Anderson (2008), *Security Engineering* (2nd edn.), p.462.
[43] Cortés et al. (2019), op. cit. endnote 10, pp.4–5.
[44] The UK in 2019 conducted trials in ten local areas requiring different types of voter identification. See UK Cabinet Office (2018), 'Next round of Voter ID pilots announced for 2019', 3 November, available at: https://www.gov.uk/government/news/next-round-of-voter-id-pilots-announced-for-2019
[45] UK Government (2019), 'The Queen's Speech 2019', 19 December, p.126, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_2019_-_background_briefing_notes.pdf
[46] Source: Darryn van der Walt (2009), Port Elizabeth, following the fourth post-apartheid South African general election, Creative Commons Attribution licence, available at: https://www.flickr.com/photos/calico182/3465337579
[47] UK Electoral Commission (2019), 'May 2019 voter identification pilot schemes', available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-research/voter-identification-pilots/may-2019-voter-identification-pilot-schemes
[48] *The Economist* (2019), 'Britain plans to require that voters show photo ID', 17 October, available at: https://www.economist.com/britain/2019/10/17/britain-plans-to-require-that-voters-show-photo-id
[49] Enrico Cantoni and Vincent Pons (2019), 'Strict ID Laws Don't Stop Voters: Evidence from a U.S. Nationwide Panel, 2008–2016', National Bureau of Economic Research Working Paper No. 25522, February.
[50] Jacob R Neiheisel and Rich Horner (2019), 'Voter Identification Requirements and Aggregate Turnout in the U.S.: How Campaigns Offset the Costs of Turning Out When Voting Is Made More Difficult', *Election Law Journal: Rules, Politics, and Policy*, Vol. 18 No. 3.
[51] Cheeseman and Klaas (2019), op. cit. endnote 32, ch.5.
[52] Cheeseman et al. (2018), op. cit. endnote 17, p.1405.
[53] Anna C Rader (2016), 'Politiques de la reconnaissance et de l'origine contrôlée: La construction du Somaliland à travers ses cartes d'électeurs' ['The Politics of Recognition and Authenticity: Constructing Somaliland through Voter Cards'], *Politique Africaine,* No. 144, pp.51–71 (translation by Google).
[54] Gus Hosein and Carly Nyst (2014), 'Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries', I&N Working Paper 2014/1, p.21, available at: https://www.idrc.ca/sites/default/files/sp/Documents%20EN/WP2014-1-AidingSurveillance-web-Nov21.pdf
[55] Ross Anderson (2008), Security Engineering (2nd edn.), p.478.
[56] Miriam Golden, Eric Kramon and George Ofosu (2014), *Electoral Fraud and Biometric Identification Machine Failure in a Competitive Democracy,* v.2.5, 17 December, p.1, available at: https://columbiacpseminar.files.wordpress.com/2015/04/golden-kramon-ofosu.pdf
[57] Cheeseman and Klaas (2019), op. cit. endnote 32, pp.67–68.
[58] Madhavan Somanathan (2019), *India's electoral democracy: How EVMs curb electoral fraud*, Brookings Institution, 5 April, available at: https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/
[59] PTI (2013), 'Supreme Court asks Election Commission to introduce paper trail in EVMs', *India Today*, 8 October, available at: https://www.indiatoday.in/india/north/story/supreme-court-asks-election-commission-to-introduce-paper-trail-in-evms-213615-2013-10-08
[60] Dhananjay Mahapatra (2019), 'Count VVPAT slips of five booths in each assembly seat: SC', *The Times of India*, 9 April, available at: https://timesofindia.indiatimes.com/india/count-vvpat-slips-of-5-booths-in-each-assembly-seat-sc/articleshow/68786810.cms
[61] Drew Desilver (2016), 'On Election Day, Most Voters Use Electronic or Optical-Scan Ballors', Pew Research Center, 8 November.

[62] Eric Geller, Beatrice Jin, Jordyn Hermani and Michael B Farrell (2019), 'The scramble to secure America's voting machines', *Politico*, last updated 12 November 2019, available at: https://www.politico.com/interactives/2019/election-security-americas-voting-machines/
[63] National Academies of Sciences, Engineering, and Medicine (2018), *Securing the Vote: Protecting American Democracy,* The National Academies Press, Washington, DC, pp.77–78, available at: https://doi.org/10.17226/25120
[64] Cortés et al. (2019), op. cit. endnote 10, p.6.
[65] Marie O'Halloran and Michael O'Regan (2010), 'E-voting machines to be disposed of', *The Irish Times*, 6 October, available at: https://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193
[66] National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.80
[67] National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.39, p.43: 'Research suggests that DRE VVPATs tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs. See, for example, SP Everett, 'The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection', doctoral dissertation, Rice University, Houston, Texas; and Bryan A Campbell and Michael D Byrne (2009), 'Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability', *Proceedings of EVT/WOTE*, 2009.'
[68] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang and J Alex Halderman (2020), 'Can Voters Detect Malicious Manipulation of Ballot Marking Devices?', Proc. 41st IEEE Symposium on Security and Privacy, Oakland '20, San Francisco, May.
[69] National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.79
[70] Bundesverfassungsgericht, Docket Nos. 2 BvC 3/07 & 2 BvC 4/07, 2009. Translation by National Democratic Institute, available at: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany
[71] Cheeseman et al. (2018), op. cit. endnote 17, p.1409.
[72] Alexander J Martin (2018), 'Government rejects online voting for disabled voters amid electoral fraud fears', Sky News, 3 September, available at: https://news.sky.com/story/government-rejects-online-voting-for-disabled-voters-amid-electoral-fraud-fears-11489389
[73] Royal National Institute of the Blind, 'Turned Out 2017', available at: https://www.rnib.org.uk/sites/default/files/Turned%20Out%202017%20APDF_1_0.pdf
[74] Andrew Ellis, Carlos Navarro, Isabel Morales, Maria Gratschew and Nadja Braun (2007), *Voting from Abroad: The International IDEA Handbook*, Handbook Series, International Institute for Democracy and Electoral Assistance, 26.
[75] More information is available on the website of the Election Commissioner of India, available at: https://eci.gov.in/divisions-of-eci/it-applications-etpbs-servicevoter/
[76] Swiss Info (2019), 'Three cantons seek damages for failed e-voting system', 8 July, available at: https://www.swissinfo.ch/eng/swiss-post_three-cantons-seek-damages-for-failed-e-voting-system/45083860
[77] Bart Jacobs and Wolter Pieters (2009), 'Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment', in Alessandro Aldini, Gilles Barthe and Roberto Gorrieri (eds.), *Foundations of Security Analysis and Design V,* Springer Berlin Heidelberg, Vol. 5705 DOI: 10/dk7qdp; G Schryen and E Rich (2009), 'Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland', 4(4), IEEE Transactions on Information Forensics and Security 729 DOI: 10/dr9676.
[78] Estonian National Electoral Committee and the State Electoral Office (2019), 'Statistics about Internet voting in Estonia', available at: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia (accessed 22 July 2019).
[79] National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, pp.101–106.
[80] See *Ch. Nasir Iqbal and others v Federation of Pakistan thr. Secy. Law and others* (PLD 2014 SC 72).
[81] *Miss Yasmin Khan and another v Election Commission of Pakistan, Islamabad through Secretary and another* (1994 SCMR 113).
[82] *Ch. Nasir Iqbal and others v Federation of Pakistan through Secretary Law and others* (Const. P. 39/2011); *Imran Khan, Chairman, PTI, etc. v Federation of Pakistan* (Const. P. 90/2011).
[83] Elections Act (Pakistan) 2017, s 94.
[84] Election Commission of Pakistan (2019), *Report on I-Voting Pilot Test in 35 Constituencies Held on 14th October 2018,* Election Commission of Pakistan, Islamabad, p.5.
[85] Elections Act 2017, s 94.
[86] See *Farhat Javed Siddique and others v Government of Pakistan* (Const. P. 74-79/2015, 49-56/2016, 2/2018, Civil Misc. Apps. 4292/2017, 162/2018); Elections Act 2017, s 239.
[87] ECP Notification S.R.O. 1166(I), 28th September 2018.
[88] Elections Act 2017, s 69.
[89] Calculated by one of the authors from electoral data as an illustrative indication, following discussion in interviews with officials – do not cite as an official statistic.
[90] See, generally, NADRA, 'International Projects', available at: https://www.nadra.gov.pk/international-projects/.
[91] ECP Order of April 19, 2018 (F No 6(1)/2011-IT), p.3.
[92] Internet Voting Task Force (IVTF) (2018), *Findings and Assessment Report of Internet Voting Task Force (IVTF) on Voting Rights of Overseas Pakistanis*, Election Commission of Pakistan, Islamabad.

[93] ECP Order of April 19, 2018 (F No 6(1)/2011-IT).
[94] Elections Act 2017, s 94; Constitution of Pakistan, art 226.
[95] See https://www.youtube.com/watch?v=iFpmUaefD34 and https://www.youtube.com/watch?v=7JWEaHCg4ns for the English versions.
[96] Election Commission of Pakistan (2019), op. cit. endnote 84.
[97] Survey.
[98] Interview with OSCE/ODIHR Long-Term Observer, Alex Folkes, 13 November 2019.
[99] Many of these tweets can be read by searching for the hashtag #IDOX (last accessed 3 January 2019).
[100] Jim Waterson, Hilary Osborne and agencies (2019), 'BBC denies Laura Kuenssberg's postal vote comments broke law', *The Guardian*, 11 December, available at: https://www.theguardian.com/media/2019/dec/11/bbc-denies-political-editors-postal-vote-comments-broke-law
[101] Center for Internet Security (CIS) (2018), *A Handbook for elections infrastructure security*, February, p.29, available at: https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[102] Cheeseman and Klaas (2019), op. cit. endnote 32, pp.177–179.
[103] Brown and Lee (March 2019), Interviews with the Electoral Commission of Ghana.
[104] Cheeseman et al. (2018), op. cit. endnote 17, pp.1405–1406.
[105] Ibid, p.1407.
[106] HM Treasury (2015), *The Aqua Book: Guidance on Producing Quality Analysis for Government*, HM Government.
[107] Brown and Veale (March 2019), Interviews with the Electoral Commission of Pakistan.
[108] Luke Tyburski (2019), 'Malawi's Election Was Not Stolen With White-Out', *Foreign Policy*, 1 November, available at: https://foreignpolicy.com/2019/11/01/malawis-election-was-not-stolen-with-white-out/
[109] Cheeseman et al. (2018), op. cit. endnote 17, p.1408.
[110] Andy Greenberg (2017), 'Everything We Know About Russia's Election-Hacking Playbook', 8 June, available at: https://www.wired.com/story/russia-election-hacking-playbook/
[111] BBC News (2017), 'Venezuela vote: Turnout figure "tampered with"', 2 August, available at: https://www.bbc.co.uk/news/world-latin-america-40804812
[112] Girish Gupta (2017), 'Exclusive: Venezuelan vote data casts doubt on turnout at Sunday poll', Reuters, 2 August, available at: https://www.reuters.com/article/us-venezuela-politics-vote-exclusive-idUSKBN1AI0AL
[113] Tom Wilson, David Blood and David Pilling (2019), 'Congo voting data reveal huge fraud in poll to replace Kabila', *Financial Times*, 15 January, available at: https://www.ft.com/content/2b97f6e6-189d-11e9-b93e-f4351a53f1c3
[114] Tom Calverley (2020), 'Congolese torture survivor gets Home Office reprieve', *The Guardian*, 15 January, available at: https://www.theguardian.com/politics/2020/jan/15/congolese-torture-survivor-gets-home-office-reprieve
[115] IDEA (2015), op. cit. endnote 4, p.19.
[116] Cheeseman and Klaas (2019), op. cit. endnote 32, p.237.
[117] IDEA (2015), op. cit. endnote 4, p.46

Chapter 3 Overarching best practices for secure elections

The use of new technology in the electoral process offers many ways to improve the efficiency and accuracy of electoral planning, voting registers and results reporting; new ways for EMBs and candidates to communicate with voters; and new mechanisms for transparency. But even with careful planning and management, it also introduces cybersecurity risks which must be carefully managed if they are not to have the potential to significantly damage public trust in election outcomes. The cybersecurity measures taken in response should obviously be proportionate to the risks introduced.

In this final part of the guide, we describe overarching best practices, not specific to any point in the electoral cycle, in assessing and managing cybersecurity risk. They are based on existing literature, a detailed survey of Commonwealth governments, and in-depth country assessments and in-person interviews carried out in four Commonwealth countries (*Pakistan*, *Ghana,* the *UK*, and *Trinidad and Tobago*). We have identified five key areas: holistic action; international co-operation; cybersecurity risk management; privacy and data protection; and action against disinformation online.

Where there is a clear, well-evidenced need – such as faster reporting of preliminary results in *Pakistan* and *Ghana*, easier voter registration in the *UK*, or piloting remote voting where consular infrastructure is lacking and postal voting is felt to be inadequate, as in *Pakistan* – there may be a strong case to introduce technology that brings with it additional cybersecurity risk. This need must be then weighed against these risks, with all appropriate mitigation measures taken and the overall risk–benefit explicitly appraised.

Without this careful assessment, digital technologies 'may create significant opportunities for corruption that (among other things) vitiate their potential impact… precisely because new technology tends to deflect attention away from more "traditional" strategies, the failure of digital checks and balances often renders an electoral process even more vulnerable to rigging than it was before'.[1]

Barbados' Elections and Boundaries Commission has created its own Electoral Management System and digitised its processes for voter registration and the update of records. It has also installed a chatbot on its website to disseminate information to voters, such as polling times and locations, and has integrated with various other chatbots such as Apple Siri, Amazon Alexa and Google Assistant to disseminate information to voters. None of *Antigua and Barbuda*'s electoral processes are online, but it is in the early stages of digitisation. It is looking to introduce the use of mobile applications and e-processing during the next two electoral lifecycles.

Recommendation 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.

Risk assessment tools help organisations 'identify, estimate, and prioritize risk' to assets, personnel, customers and other organisations. They assess potential threats, vulnerabilities, harm and likelihood of harm, and at the technical level are used to select 'security categorization; security control selection, implementation, and assessment; information system and common control authorization; and security control monitoring'.[2]

These tools can be used by EMBs to assess new technologies and systems, to consider: whether their risks overall are manageable before approving their use; the security mechanisms needed to manage that risk; and the residual risks that remain. The US federal government agency NIST (National Institute of Standards and Technology) identifies the following activities that can be supported by a risk assessment:

- development of an information security architecture;
- definition of interconnection requirements for information systems (including systems supporting mission/business processes and common infrastructure/support services);

- design of security solutions for information systems and environments of operation, including selection of security controls, information technology products, suppliers/supply chain and contractors;
- authorisation (or denial of authorisation) to operate information systems or to use security controls inherited by those systems (i.e., common controls);
- modification of missions/business functions and/or mission/business processes permanently, or for a specific timeframe (e.g., until a newly discovered threat or vulnerability is addressed, until a compensating control is replaced);
- implementation of security solutions (e.g., whether specific information technology products or configurations for those products meet established requirements); and
- operation and maintenance of security solutions (e.g., continuous monitoring strategies and programmes, ongoing authorisations).[3]

These tools differentiate between vulnerabilities – weaknesses in systems or procedures that can be exploited; threats – circumstances that can adversely affect an organisation, from threat sources such as hostile attacks, mistakes, structural failures and natural disasters; likelihood – the probability a given threat will exploit a specific vulnerability; and impact – the level of harm that would result.[4]

Commonly used risk assessment tools include the following:

- COBIT 5 for Risk & Risk Scenarios – a business-focused framework for managing and governing enterprise information system risk, with sections on the enterprise risk function and how to identify, analyse, respond to and report on risk on a daily basis.[5]
- The Factor Analysis of Information Risks (FAIR) methodology, a more quantitively focused risk analysis methodology, enabling the modelling of value at risk.[6]
- NIST Special Publication 800-30 – freely available guidance, mandated for use by US federal agencies (other than national security systems). Because of its wide use in the US government, business and software support is more readily available than other frameworks.[7]

Box 3.1 Risk management tools and approaches

Such mitigation measures will often have two core dimensions.[8] They will in general consist of a combination of:

- prevention, such as through deterring the antagonist and reducing exploitable vulnerabilities; and
- mechanisms for limitation of interference and effect, such as early warning and detection systems, co-ordination forums, and education and exercises to promote efficient and effective action.

The overarching strategies we suggest in the following section are designed to support effective prevention and limitation of adverse impact across the areas EMBs have responsibility for. They are also intended to build voter confidence in technologies used in electoral processes. Without demonstrated effective cybersecurity measures, allegations of breaches or hacking can be as damaging to trust in electoral processes as actual incidents.

3.1 Holistic action

Managing cybersecurity risks in elections requires cross-government co-ordination and a legal framework that addresses all stages of the electoral cycle – including areas such as data protection that may traditionally have been outside the remit of EMBs.[9]

To facilitate cross-government co-operation, *Botswana* has set up an election task force made up of Ministries of the Interior, Defence and Justice. In *India*, multiple agencies contribute to election cybersecurity, including the national Critical National Infrastructure Centre, CERT-India and the National Informatics Centre. They all provide information to the co-ordinating EMB. In the *EU*, the European Commission has recommended a co-ordinating

committee. Some EU countries have done this through the prime minister or president's office, while other initiatives have been more independent of government, via the EMB.

In Trinidad and Tobago, the issue of cybersecurity is overseen by an inter-ministerial advisory committee, which produced the government's National Cyber Security Strategy in 2012 to guide all operations and initiatives related to cybersecurity. In the context of elections, its relevant objectives are the protection of the physical, virtual and intellectual assets of citizens, organisations and the state; the prevention of cyber-attacks against critical infrastructure; and the provision of a governance framework to identify the requisite organisational structures necessary for cybersecurity.[10]

Cybersecurity is now a high priority of the Ghanaian government and is overseen by an inter-ministerial advisory committee and the National Cyber Security Technical Working Group, which comprises all relevant government and external stakeholders. The Ministry of Communications (MOC) is tasked with implementing cybersecurity policy and strategy, which it was in the process of reviewing at the time of writing. It was also drafting cybersecurity legislation to address identified weaknesses in its cybercrime laws and will make provisions for appropriate sanctions and non-compliance.

Box 3.2 Cross-government decision-making in Trinidad and Tobago and Ghana

Different Commonwealth countries have different constitutional and legal limits on how far EMBs may delegate such issues to other government agencies. And some EMBs, such as the *United Kingdom's*, have limited powers outside of electoral periods, whereas others, like *Antigua & Barbuda's*, have constitutional authority to oversee all aspects of the elections, leaving limited scope for initiatives led by other regulators.

The New Zealand Electoral Commission is working closely with support agencies across its wider government sector to help plan for and mitigate security risks for the NZ general election in 2020. A key component of this work includes setting up a governance structure involving the support agencies sitting alongside the commission to help it manage risks relating to the delivery of a critical public event. The governance approach will use shared risk identification, scenario planning and cross-agency protocols to form a platform for a cross-agency team to mitigate risk and respond to any issues that might arise during critical periods.

The New Zealand Commission has been working with international partners to understand and learn from approaches taken in recent elections, in particular with the Australian Electoral Commission which implemented a cross-agency model (called the 'Election Taskforce') leading up to and during Australia's federal general election in May 2019.

Box 3.3 New Zealand cross-agency working

EMBs also need to co-ordinate cybersecurity measures with parties and campaigners, private sector suppliers, the media and civil society groups – including educating voters. As the North Atlantic Treaty Organisation (NATO) observed in 2019:

> Protecting elections is a multilayer and multistakeholder process that necessitates the development of new coordination mechanisms, new methods and tools to monitor and assess the information environment, improved routines for risk and vulnerability analysis and a framework to assess and respond to election interference.[11]

These measures will ensure all relevant organisations are building their own cybersecurity capabilities and resilience; are contributing their own expertise; and will understand the cybersecurity measures EMBs may take at short notice during an election period, maintaining their perceptions of EMB impartiality. NATO has noted approvingly that 'the positive effects of NGOs [non-governmental organisations] and civic society organisations' willingness to ensure full transparency of electoral processes, including the influencing of voters' choices, have helped ensure a high level of resilience'.[12]

Recommendation 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.

The media has an important role to play in the conduct of Ghanaian elections, particularly in light of the new modern media landscape. Its complexity is increasing, with the Ghana Journalist Association (GJA) estimating that the number of radio stations has doubled to 400, TV stations has increased from 30 to 200 stations, and that there are now over 1,000 newspapers operating in Ghana. Social media and citizen journalism are also growing in importance and are redefining the boundaries of the profession, and there is a need for traditional media to respond.[13]

There are concerns in Ghana around the rise of new media and its potential to facilitate the spread of misinformation. The National Communications Authority (NCA) is partnering with the National Media Commission (NMC) to jointly produce guidelines on general election news and reporting for 2020, issues which have proved incendiary in the past. If the 2020 election is subject to any foreign interference or cyber-attack, then the media will have to be part of any holistic response, to increase trust in the use of technologies and to counter any misinformation.

The NMC, the Ghanaian Institute for Public Relations (IPR) and the NCA have suggested improved electoral training for journalists and information officers, to take account of the modern election environment. The GJA is similarly considering updating its guidelines, which in 2016 highlighted risks to the security of news outlet's own systems. It stated that: 'Media houses are to bear in mind that while information and communications technology tools can help enhance journalism, there are security threats and the risk of their sites being tampered with. Media houses and journalists operating in this area are therefore advised to develop capacity in the effective use of the technology and to use reliable software'.[14]

Box 3.4 Ghana's media environment

Recommendation 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 carefully consider any differential impact of the digitisation of electoral processes, and associated cybersecurity measures, on different groups such as men and women, urban and rural voters, manual and non-manual workers, and visually impaired or otherwise disabled persons. Literacy rates, let alone basic digital skills and internet access, often vary significantly between these groups; as does the likelihood of successful fingerprint registration.

In the Commonwealth, only one third of children in developing countries has access to early childhood education, approximately 17 million primary children remain out of school, and more than 400 million adults are illiterate. And the stark reality facing many of our Commonwealth member countries is that they are having to find funds to maintain and improve education services on shoestring budgets and sometimes after having their entire economy wiped out by a natural disaster.[15]

Recommendation 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.

3.2 International co-operation

The ease with which attacks can be carried out remotely against information systems, and with which vulnerabilities and attack tools can be developed and shared between countries and in online criminal marketplaces, means that international co-operation is key in

responding to attacks on election cybersecurity. For example, in West Africa, it was reported that

> following raids on cyber cafés in major cities in Nigeria, cybercriminals were reported to move to remote areas to carry out their operations. The porous national borders and a lack of countries' controls on their territories allow cybercriminals to migrate to jurisdictions with a weaker rule of law [..] In 2008, 40% of arrested cybercrime suspects in Ghana were Nigerians, 38% were Ghanaians and the rest were from Liberia, Cote d'Ivoire and Togo.[16]

Co-operation allows countries – especially smaller Commonwealth members – to collectively build a much stronger and most sophisticated capability to defend against attacks compared to acting alone. The Commonwealth 2018 Cyber Declaration emphasises the importance of this co-operation and the Commonwealth Secretariat is already setting up a platform to support this. NATO has also noted: 'While national preparations can be very ambitious, the lack of awareness and detailed understanding of the approaches taken can result in unhelpful reactions on the part of neighbouring countries or partners'.[17]

Central databases of resources, like International IDEA's lists of election tool components, reviews, certifications and approved certification bodies,[18] will help EMBs find relevant information. Background data such as titles and links to relevant laws (elections, data protection, cybersecurity) and treaties could be usefully shared between Commonwealth countries, populated initially from our survey.

EMBs face many common cybersecurity threats, in terms of attackers interested in disrupting elections and particularly **vulnerabilities** in the systems they use. EMB co-operation to share relevant information across the Commonwealth, and with regional organisations such as CARICOM, would improve the efficiency and timeliness of their response. Free tools to support this, such as Malware Information Sharing Platform (MISP),[19] are available. Peer learning via **regional hubs** with the participation of major cybersecurity agencies, such as those of the UK and Singapore, would be one possible institutional mechanism. Such hubs may be able to develop shared services, such as election security operations centres for small states that would otherwise find this a very resource-intensive task. Peers could also provide independent review of cybersecurity policies.

Cybersecurity co-operation does, however, remain challenging for some EMBs, who must avoid the perception of international regulatory capture, particularly where electorates commonly express distrust about electoral governance or where international tensions exist. Co-operation should be carried out openly and clearly, with clear tasks and reasons for such co-operation, to ensure that public trust is not endangered.

One area of elections where countries already co-operate extensively is election observation missions. Organisations (including the Commonwealth) which co-ordinate such missions need to further develop cybersecurity indicators that can be integrated into their regular observations. The Organization for American States (OAS) has produced a detailed guide to gathering this information.[20] The importance of this can be seen in the preliminary results from a recent OAS observation mission to *Bolivia*, which led to the election being suspended, and then to a change of government.[21]

> An Organization of American States team of 36 specialists, including IT experts, observed the Bolivian general elections held throughout the country on 20 October 2019. The team audited the following:
>
> 'A. The authenticity and reliability of the vote count records (tally sheets) and of the data input into the electoral results transmission system and the official count system.
>
> B. The Plan for comprehensive custody of all electoral materials (tally sheets, ballots, voters register).
>
> C. Infrastructure and operation of the I.T. systems used to transmit preliminary results and the official count.
>
> D. Uploading flows of the data on preliminary electoral results and the official count.'
>
> The team found serious problems with the preliminary election results transmission system (TREP). It detected one TREP server being used for a different purpose to that previously notified, without a corresponding monitoring agent, and the redirection at 7.40pm on election day of results

information to another server that had not been notified at all – and which was being controlled by an external person. Logs differed on election servers without any explanation. Metadata from the smartphone camera images of tally sheets received via the results service was not kept, while tally sheets were received with dates not matching the election. No hash value was stored of the software running on the results servers when it was frozen for the election, while not all of the data flows to the results servers were monitored. The team therefore concluded: 'It is not possible to certify the accuracy of the TREP'.

The team further found that '[b]est practices were not followed' in the official count. Unit, integration and regression testing was not carried out, nor was there a formal software acceptance process. User authentication was weak, and the database reset process 'did not follow basic security requirements'. Software was recompiled during the count and put straight into use. Test data was not removed before the count and was found 'mixed up with Election Day tally sheets', while preliminary tally sheets found their way into the official count. The app provider had direct remote access to the server, which needed to be used by the head of the company to fix a programming error, and critical electronic evidence was not kept. The app provider broke the chain of custody. These multiple errors led the OAS team to conclude 'it is impossible to guarantee the integrity of the data and certify the accuracy of the results'.

There were other serious issues, including forged signatures on tally sheets, while 38 per cent of tally sheets checked were 'inconsistent with the number of citizens casting a vote'. The vote leapt by over 15 per cent for the governing party in the final 5 per cent of votes counted, avoiding the need for a run-off election. The team concluded: 'The manipulations of the I.T. system are of such magnitude that they should be investigated in depth by the Bolivian State in order to get to the bottom of them and determine who is responsible for such a serious situation… The audit team cannot validate the results of this election and therefore recommends another electoral process. Any future process should be overseen by new electoral authorities to ensure the conduct of credible elections'.

Box 3.5 OAS preliminary audit of the Bolivian presidential elections on 20 October 2019

Recommendation 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.

Recommendation Electoral observation teams should include the technical expertise needed to effectively monitor digitised electoral processes.

EMBs can also promote awareness among their stakeholders of relevant international initiatives – for example, the Alliance of Democracies' Pledge for Election Integrity, which has been signed by nearly 200 European and North American politicians.[22] Other organisations, such as the civil society group Asian Network for Free Elections (ANFREL), Caribbean Telecommunications Organisation and the Association of Southeast Asian Nations (ASEAN) are also emerging as venues for co-operation. And EMBs also co-operate informally – for example, with regular meetings between the electoral commissions of the *UK*, *Canada*, *Australia* and *New Zealand*.

Recommendation 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).

Recommendation EMBs should develop mechanisms to enable information sharing across the Commonwealth on threats, vulnerabilities and detected attacks against election infrastructure.

Recommendation 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).

Recommendation Commonwealth EMBs should provide peer support and review on cybersecurity to their neighbouring EMBs, as well as sharing training opportunities.

3.3 Cybersecurity risk management

Having carried out a threat assessment, EMBs will then be in a good position to undertake a proportionate risk management programme to protect the systems that are key to a trustworthy election process against the identified threats. This will likely involve the national cybersecurity centre or equivalent public sector centre of expertise.

EMBs need to plan how to develop their long-term cybersecurity capacity through training and efficient mechanisms for procuring private-sector cybersecurity services. To build public confidence, they should consider how security-critical systems can be certified and quality assured. And EMBs should carefully plan the audit trails provided by all of their systems, to enable disputed election results to be investigated and fairly decided.

A key part of this risk management approach is considering how far election outcomes are dependent upon digital systems. Where hand-marked and counted paper ballots are used as the definitive record, cybersecurity risk in the voting process is significantly reduced, with an audit trail that can be forensically examined and adjudicated in a way that commands broad public confidence. Where electoral rolls are a matter of public record, and can be challenged by parties, the risk of manipulation is reduced. Where candidates and the media can observe and publicise count results, the risk of interfering in outcome reporting is also reduced. The *Canadian* government assessed the relative risk in 2019:

> Cyber threat activity very rarely affects the IT systems that electoral agencies use for recording, storing, and transmitting election data, such as the vote count. Such activity accounted for less than four percent of all cyber threat activity against elections globally in 2018. Cyber threat actors very likely see changing a vote count in a national election as difficult and very likely consider it impossible against elections that use hand-counted paper ballots, such as the Canadian federal election.[23]

That said, attacks on electoral systems still have the potential to cause significant confusion, delay, and damage public confidence in both the results and the competence of electoral authorities. Where electronic voting machines are used, or biometric authentication is used to verify voters, risks are significantly higher – and hence proportionately greater risk management measures will be required.

National cybersecurity centres and strategies

Most Commonwealth countries now have national cybersecurity centres, computer emergency response teams (CERTs), computer security incident response teams (CSIRTs) or equivalents. These bodies will be the government's centre of cybersecurity expertise, and important partners for EMBs in securing election systems.

In some countries, such as *Ghana* and *Trinidad and Tobago*, these centres play a mandatory role in securing systems the government has designated as critical national infrastructure (CNI). In *India*, where election systems have been declared to be CNI, the EMB may consequently create security regulations – and was the first CNI agency to do so. Network security and data centres are managed by other national agencies.

Recommendation EMBs and national cybersecurity agencies should consider whether designation of key election systems as part of critical national infrastructure will improve their security.

Cybersecurity centres also commonly produce national cybersecurity strategies to reduce risk across the whole of society, which is important for elections, given that they potentially involve almost every adult in the country.[24]

An important consideration in partnerships between EMBs and these government centres is the need to protect EMB **independence,** where provided for in statute or national constitutions, such as in *Ghana* and *Pakistan*.[25] Given the links between national cybersecurity agencies and intelligence agencies, this can be challenging, particularly in countries where some political actors treat intelligence agencies with suspicion. This may explain why the

majority of respondent Commonwealth EMBs (54%) do not have a partnership with their national cybersecurity centre or CERT. Figure 3.1 shows that this is not consistent across the different types of Commonwealth countries, where 83 per cent of high-income country EMBs but only one small island developing country EMB have these partnerships in place. A related issue is the extent to which EMBs make use of shared government IT services. *Jamaica*'s electoral processes run on an isolated network and separate virtual private networks (VPNs) are used for each of the Electoral Commission's offices, but the country is looking into central integration with the government's networks.

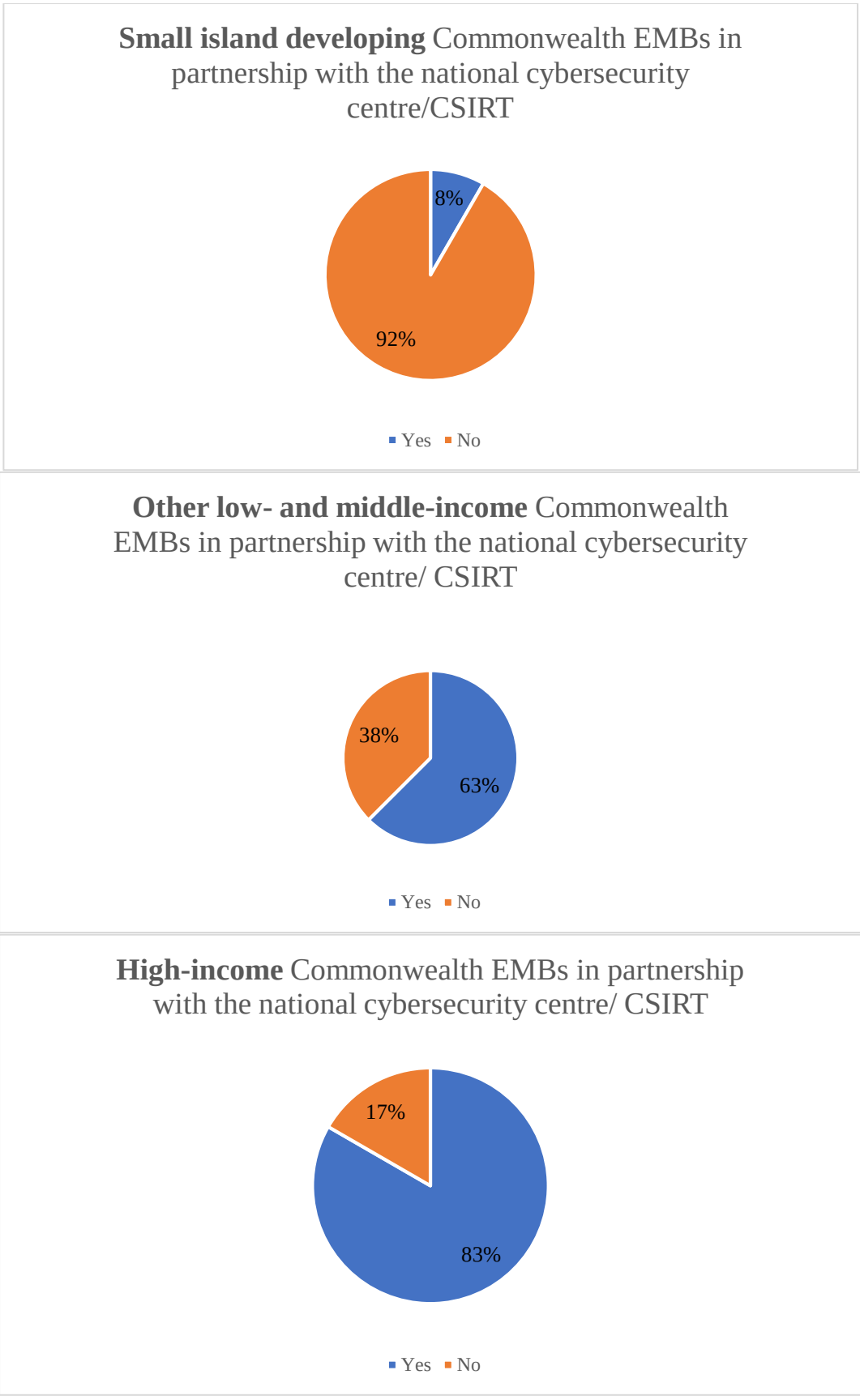


Figure 3.1 Proportion of respondent Commonwealth EMBs which have a partnership with the national cybersecurity centre or CSIRT

The *UK* Electoral Commission found it easier to co-operate on information security when the government created a separate organisation (the National Cyber Security Centre [NCSC]) with this function, even while the NCSC remained part of its parent signals intelligence agency, GCHQ.

In many Commonwealth countries, some electoral functions are carried out by regional/provincial and local government. In some countries, such as the *UK*, this covers the security-critical functions of both electoral registration and polling. But these bodies do not have the cybersecurity resources of national governments and will need significant support from them to counter the serious threats they face.

Even in the *USA*, whose federal and (some) state governments are some of the most experienced and sophisticated users of information technology in the world, voluntary federal standards and advice from the Department of Homeland Security (DHS) have not been enough to fill gaping security holes.[26] Box 3.6 describes the US federal assistance being provided to state and local election officials in advance of the 2020 presidential elections.

Joint Statement from Department of Justice, Department of Defense, Department of Homeland Security, Director of National Intelligence, Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency on Ensuring Security of 2020 Elections

Attorney General William Barr, Secretary of Defense Mark Esper, Acting Secretary of Homeland Security Kevin McAleenan, Acting Director of National Intelligence Joseph Maguire, FBI Director Christopher Wray, US Cyber Command Commander and NSA Director Gen. Paul Nakasone, and CISA Director Christopher Krebs today released the following joint statement:

> Today, dozens of states and local jurisdictions are hosting their own elections across the country and, less than a year from now, Americans will go to the polls and cast their votes in the 2020 presidential election. Election security is a top priority for the United States Government. Building on our successful, whole-of-government approach to securing the 2018 elections, we have increased the level of support to state and local election officials in their efforts to protect elections. The federal government is prioritizing the sharing of threat intelligence and providing support and services that improve the security of election infrastructure across the nation.
>
> In an unprecedented level of co-ordination, the U.S. government is working with all 50 states and U.S. territories, local officials, and private sector partners to identify threats, broadly share information, and protect the democratic process. We remain firm in our commitment to quickly share timely and actionable information, provide support and services, and to defend against any threats to our democracy.
>
> Our adversaries want to undermine our democratic institutions, influence public sentiment and affect government policies. Russia, China, Iran, and other foreign malicious actors all will seek to interfere in the voting process or influence voter perceptions. Adversaries may try to accomplish their goals through a variety of means, including social media campaigns, directing disinformation operations or conducting disruptive or destructive cyber-attacks on state and local infrastructure.
>
> While at this time we have no evidence of a compromise or disruption to election infrastructure that would enable adversaries to prevent voting, change vote counts or disrupt the ability to tally votes, we continue to vigilantly monitor any threats to U.S. elections.
>
> The U.S. government will defend our democracy and maintain transparency with the American public about our efforts. An informed public is a resilient public. Americans should go to trusted sources for election information, such as their state and local election officials. We encourage every American to report any suspicious activity to their local officials, the FBI, or DHS. In past election cycles, reporting by Americans about suspicious activity provided valuable insight which has made our elections more secure. The greatest means to combat these threats is a whole-of-society effort.

Box 3.6 US Department of Justice press release on 2020 election security, 5 Nov 2019

Public sector capacity and training

A common difficulty for many government organisations is recruiting staff with cybersecurity training and experience, given the high salaries available for such jobs in the private sector. For example, in the last decade, *India* has found it 'difficult to enforce the Reserve Bank of India guidelines due to the lack of IT security auditors to validate banks' cybersecurity practices'.[27]

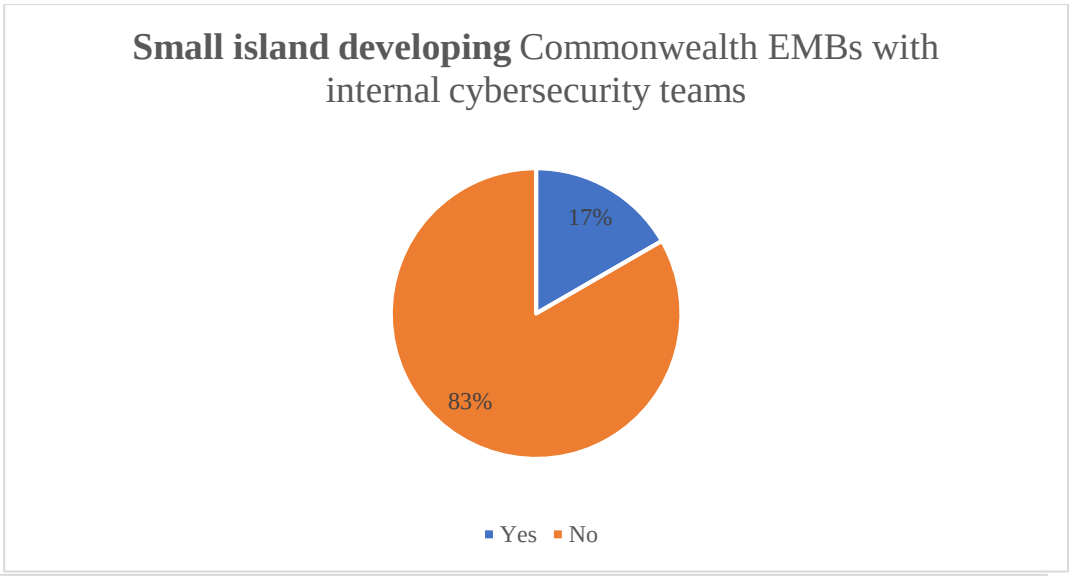
Low salaries in EMBs compared to the private sector can also introduce additional security risks, such as a higher risk of successful bribery and insider attacks. EMBs should consider how other parts of their national government that are in need of high-demand experts manage the process, such as the relaxed requirements on salary scales common in financial and competition regulators, and consider whether those measures might be applicable in their own circumstances. Our survey of Commonwealth EMBs demonstrated an alarming lack of internal cybersecurity capacity and board-level representation (even in high-income countries), as Figures 3.2 and 3.3 show.

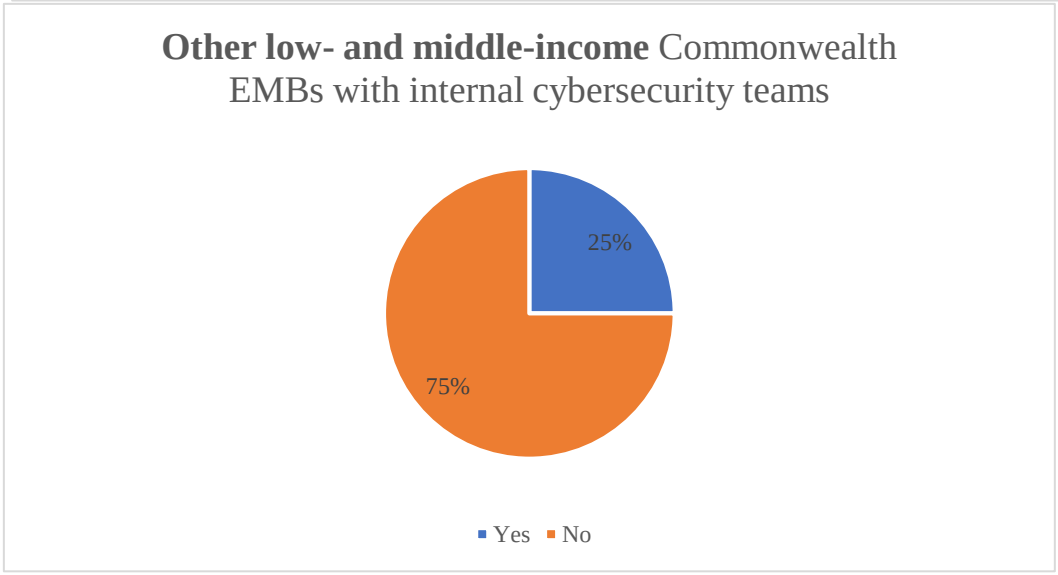
It is therefore important for EMBs to plan to build existing technical **staff capacity** through training, organisational learning and to develop a supply of future qualified staff through co-operation with universities running computer science and postgraduate cybersecurity courses.[28] Larger Commonwealth countries may have the resources to develop such training courses themselves – for example, at the Election Academy recently completed by *Pakistan's* Election Commission. Such courses can also be made available to neighbouring EMBs and non-government stakeholders such as political party staff, candidates and volunteers.

Ghana is addressing its cybersecurity skills gap via a number of initiatives. The National Cyber Security Centre is recruiting and training young promising graduates and asking them to serve in government for a minimum of five years. It is also working with the Council of Europe to develop sustainable training models. The National Communications Authority has a similar scheme for national service workers, which is demonstrating high retention rates, and the Kofi Annan Centre for Excellence together with Ghana's Technology University College are also developing cybersecurity training and encouraging young people to take it up. Additionally, the Ministry of Communications is looking at incorporating cybersecurity into the existing curriculum with the Ministry of Education, while the Ghana Investment Fund for Electronic Communications (GIFEC) is advocating the promotion of cybersecurity awareness via its work to improve connectivity in local communities.

Box 3.7 Ghana cybersecurity training initiatives

The *UK's Cyber Essentials* scheme is a good example of a broad cybersecurity programme for organisations (see Box 3.8), which is freely available for adaptation by EMBs and their partners. *Australia*'s *Strategies to Mitigate Cyber Security Incidents* provides a good, more detailed set of practices to follow.[29] The *Barbados* Elections and Boundaries Commission uses games to educate its users on the importance of cybersecurity, through the simulation of attacks on its network.





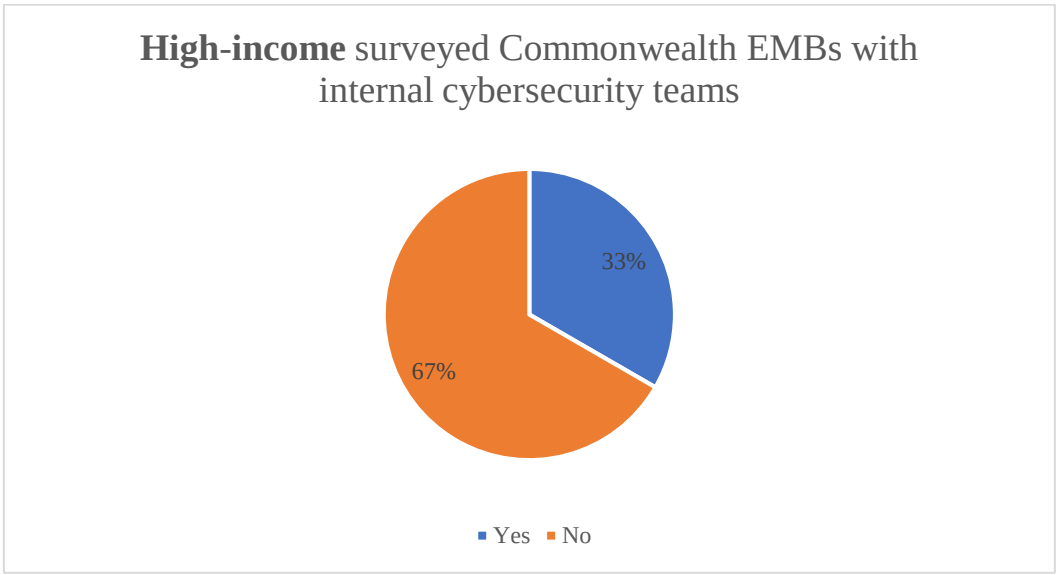
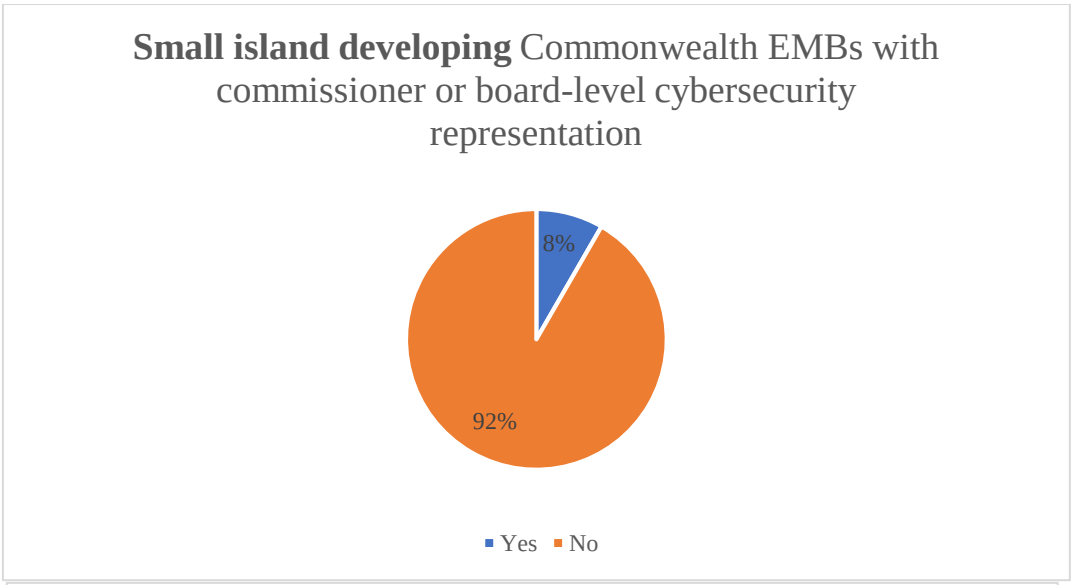
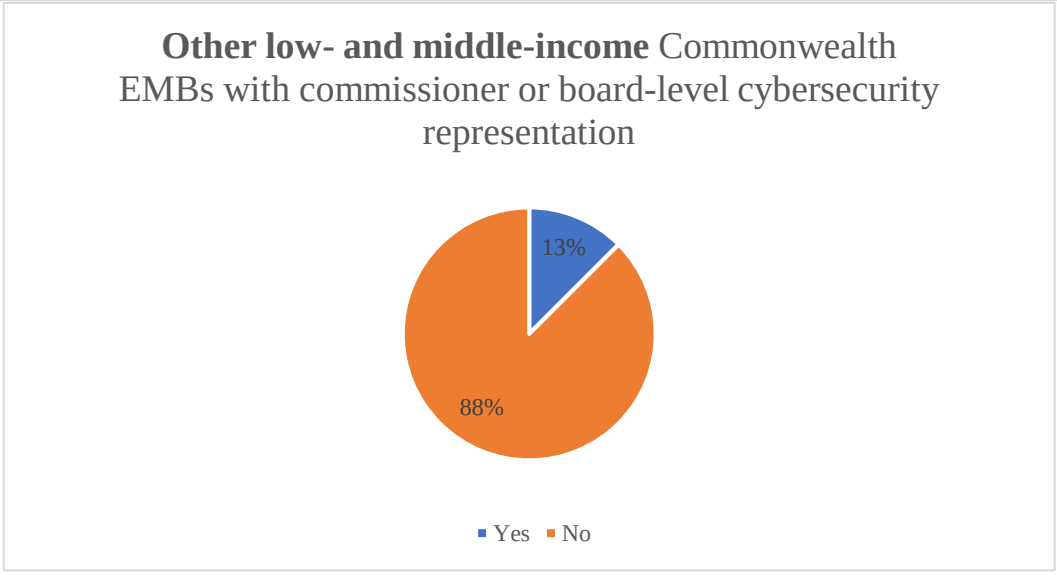


Figure 3.2 Proportion of respondent Commonwealth EMBs which have internal cybersecurity teams

The vast majority of security breaches use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the internet which enable even low-skill actors to exploit these vulnerabilities. Properly implementing basic cybersecurity hygiene (for example, using strong passwords, securing devices, not clicking on suspicious links and reporting incidents) among EMB non-technical employees will protect against the vast majority of common internet threats. Although basic cybersecurity hygiene will not stop sophisticated adversaries from compromising systems, it will dramatically mitigate risks associated with the majority of cybersecurity threats from occurring and will embed a culture of prudent information management (particularly as electoral processes further digitise).

EMBs should therefore provide all staff using computer equipment with regular basic cybersecurity training, for instance, the UK's *Cyber Essentials* (see Box 3.8), covering matters such as choosing good passwords (and important additional security such as two-factor authentication[30]), and considering social and cultural practices that might lead officials to engage in risky practices. For example, *India's* EMB has found that many returning officers, who are senior officials, see using computers as a junior data-entry operator job, and therefore share passwords and phones with their staff. The *UK*'s National Cyber Security Centre has provided a free 30-minute online training course, *Stay Safe Online: Top Tips for Staff*, which is a good starting point for non-technical staff.[31] NCSC also provides guidance on the protection of personal computers and mobile phones, as well as a range of other cybersecurity topics.[32]





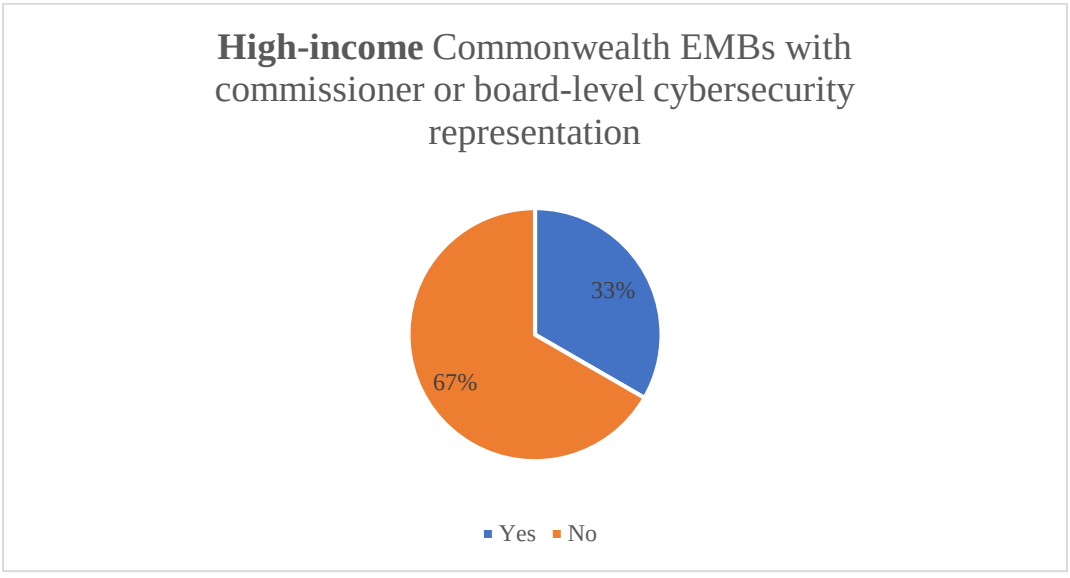


Figure 3.3 Proportion of respondent Commonwealth EMBs who have commissioner or board-level cybersecurity representation

Recommendation 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.

Cyber Essentials is a UK government-backed, industry-supported scheme to help organisations protect themselves against common online threats. The government worked with the UK Information Assurance for Small and Medium Enterprises (IASME) consortium and the UK Information Security Forum (ISF) to develop *Cyber Essentials*, a set of basic technical controls to help organisations protect themselves against common online security threats.

Cyber Essentials offers a foundation of basic cyber hygiene measures that all types of organisations can implement to significantly reduce their vulnerability. Although it is not designed to address advanced targeted attacks, *Cyber Essentials* defines a focused set of controls which will provide cost-effective, basic cybersecurity for organisations of all sizes.

Examples include: using a firewall to secure your internet connection; choosing the most secure settings for your devices and software; controlling who has access to your data and services; protecting your devices from viruses and other malware; and keeping devices/software up to date.

Cyber Essentials is suitable for all organisations, of any size, in any sector. The Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, has been designed to be achievable at low cost. The two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It should be noted, however, that *Cyber Essentials* is only a minimum level of protection and not a checklist for complete safety.

EMBs, political parties, media organisations and other electoral stakeholders can all dramatically reduce their exposure to cyber-attack if they adhere to basic cybersecurity controls.

Box 3.8 The UK *Cyber Essentials* scheme

Ongoing threat assessment

EMBs need to undertake regularly updated, comprehensive risk assessment exercises that consider the range of threats to their technical systems, identifying dependencies between critical processes, assigning probabilities to risks and assessing their consequences. This will allow EMBs to prioritise mitigation measures for vulnerabilities with higher risk, criticality and consequences.[33]

One assessment tool and testing tool developed specifically for EMBs is the IFES (International Foundation for Electoral Systems) HEAT Process (Holistic Exposure and Adaptation Testing) – which tests both election technology, and its legal and operational context. The process takes part in five phases, as shown in Figure 3.4.[34]

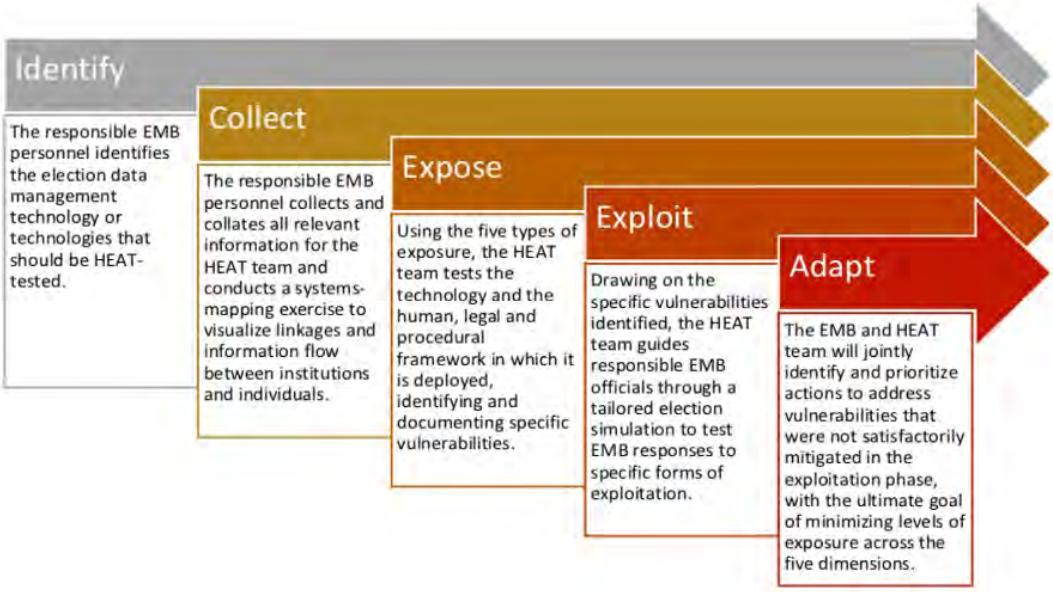


Figure 3.4 Phases of the IFES HEAT Process (Holistic Exposure and Adaptation Testing)

Recommendation EMBs should conduct comprehensive, regular threat assessments, using a tool such as the IFES HEAT Process

Procurement processes

Where EMBs rely on procuring products and services from the private sector for elections, they need to consider how to encourage the development of **effective and competitive marketplaces**. Even large Commonwealth countries such as the *UK* and *Pakistan* have limited national markets for relatively infrequent elections, and co-operation between countries on **standards** for products, certification and evaluation, and review and openness requirements for software, would encourage greater investment and competition in the private sector.[35] These standards should include secure configuration by default, along with consideration of the liability of vendors for security breaches. Collaboration will enable EMBs to obtain better terms than they could get individually – particularly in smaller Commonwealth countries. Transparency of non-prejudicial parts of contracts, as well as funding arrangements and sources of funds, would also strengthen EMBs' negotiating capabilities, as well as building public trust and reducing opportunities for corruption.

Co-operation on procurement and open source electoral software development, maintenance and support, would increase the availability and cost-efficiency of products. Where EMBs have common cybersecurity needs, such as threat intelligence and denial of service protection, they could co-operate to agree model contracts with service providers, to simplify and speed up procurement. Even obtaining secure ballot papers at scale and in good time for printing has in the past been a problem for some countries, such as *Pakistan*.

Co-ordination and co-operation must, however, be done with care, to avoid public concerns around foreign interference in elections, and to maintain as full visibility and governance of the supply chain as necessary to ensure security.

Recommendation 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.

Recommendation EMBs – and funders of election digitisation programmes – should aim for maximum transparency of contracts with suppliers, and of funding arrangements.

A number of Commonwealth EMBs have used cloud computing to support their operations. Cloud computing can be defined as a 'model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.[36] Storage, software and computing resources are hosted by a third party, whether this is a local internet service provider (ISP) or another company, in the same jurisdiction or outside (well-known providers include Amazon, Microsoft and Google). This enables EMBs to pay for computing resources when they are required, rather than having to buy and manage their own computing infrastructure, some of which may lie unused during quiet periods between elections.

Cloud computing can provide numerous benefits to EMBs at various points in the election lifecycle – such as providing day-to-day storage and editing of official documents for planning and logistics, and for public-facing services such as websites which may receive very high peak traffic during election periods. EMBs have the ability to ramp up usage or security during pressure points, such as during an election or period of registration. Large cloud storage providers have the economies of scale and access to technical expertise with which to provide more secure storage options than can be developed in-house, particularly in the case of smaller EMBs.

The storage of data by large providers in centres abroad has raised issues of trust, security and foreign interference. EMBs can consider requiring suppliers to domicile sensitive data locally.

A variety of approaches have been taken in Commonwealth EMBs, according to national contexts and the relative strengths of local IT industries. The issue has been topical, particularly in the Asia-Pacific region.[37] Australia, for example, uses Amazon Web Services (AWS) to provide public-facing services and services for electoral administrators. It also has rules around the local storage of data to ensure data sovereignty. In South Africa, the results website is hosted by a local ISP to ensure scalability for the high volumes and provide additional layers of security. Pakistan, however, faces electricity and connectivity constraints in rural areas, so has taken a different approach.

Cloud computing can prove more challenging for small island states with limited global internet connectivity, for example, in Samoa, where the EMB decided not to transition to the cloud to preserve data sovereignty. However, some EMBs reported interest in using cloud services for internal operations, such as the Tongan EMB.

Box 3.9 Commonwealth EMB use of cloud computing

Certification and quality assurance

One important mechanism for building public trust in election technologies is to follow international standards in their testing – for example, the widely used ISO 27000 series (see Box 3.10), although that is a highly resource-intensive process and reliant on the availability of thorough (and expensive) third party evaluators. Nonetheless, 74 per cent of respondent Commonwealth countries do not use international standards in the development of policies, regulations or processes for elections cybersecurity. Figure 3.5 shows the breakdown of adoption across high-income, middle- and low-income, and small island developing Commonwealth countries.

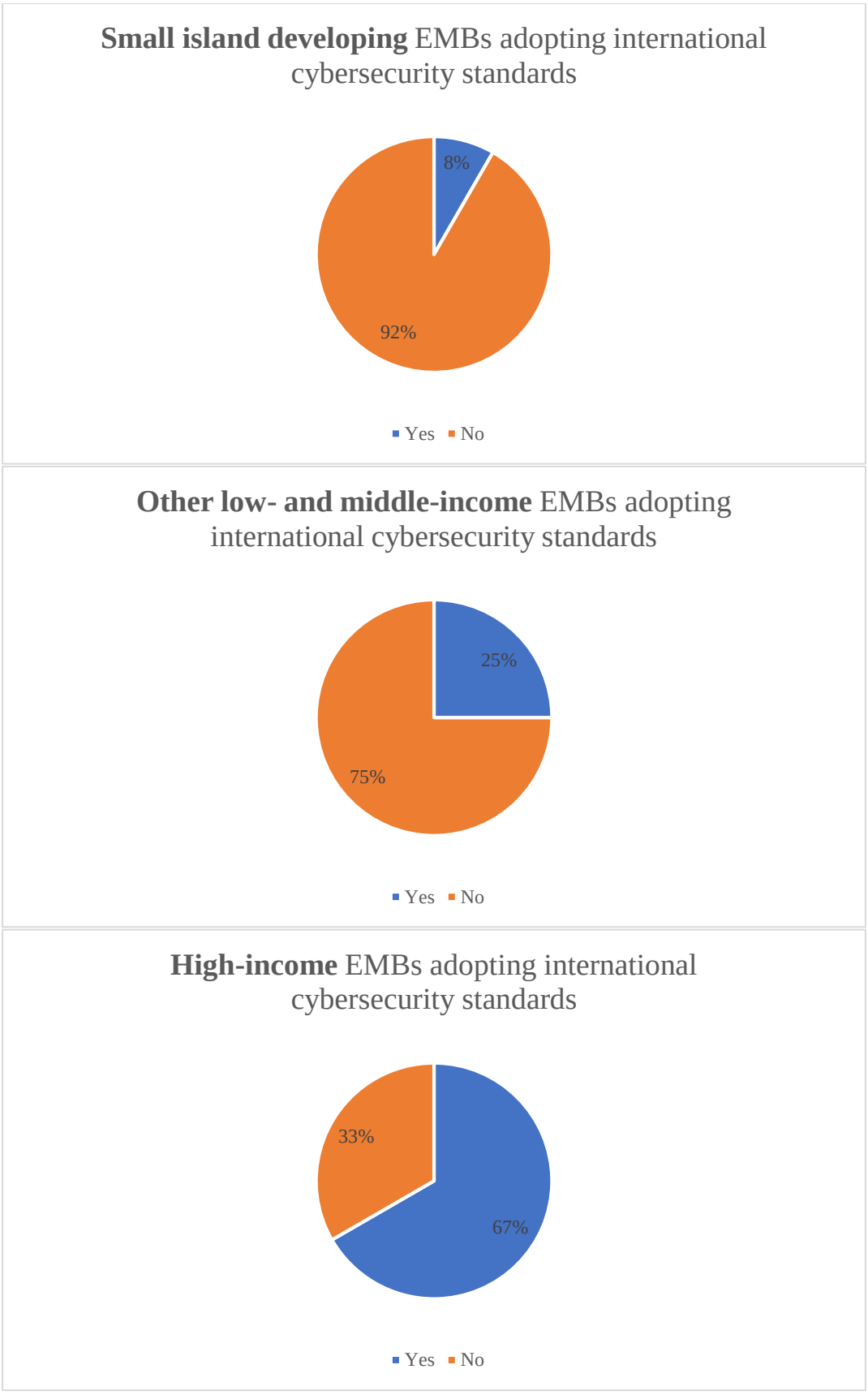


Figure 3.5 Proportion of EMBs which have used international standards (such as those developed by ISO, IEE, the UN, OAS, etc.) in the development of policies, regulations or processes for elections cybersecurity

The most widely used series of information security standards is published jointly by the International Organization for Standardization and the International Electrotechnical Commission and is known as the ISO/IEC 27000 series. It provides regularly updated and comprehensive best practice recommendations on developing and implementing an information security management system (ISMS).[38] It also allows independent third parties to assess the quality of an organisation's ISMS – which could be particularly useful to EMBs looking to build public confidence in high-risk elements of their electoral technology systems.

This is the approach taken by the Election Commission of Pakistan, which works with Pakistan's National Database and Registration Authority to maintain strict information security standards, such as certification of their data warehouse and network against ISO/IEC 27000, with external audits. The Electoral Commission of Ghana has also based its cybersecurity policy on ISO/IEC 27000.

The ISO/IEC 27000 standard series requires extensive assessments and documentation of systems, and hence is resource intensive. Some of our interviewees also felt the series focuses more on processes than security measures. The quality of external audits depends on the skills and experience of the auditors used – this is a specialised field and smaller countries (especially those lacking a significant financial sector, the largest users of these standards) might have a limited choice of qualified auditors. India's electoral commissioners have also been unwilling to reveal some of the internal information required for the process of external certification.

In the UK, the Electoral Commission has assessed that the cybersecurity risk associated with its political party registration and funding oversight systems is best managed using the lower-overhead UK National Cyber Security Centre's *Cyber Essentials* scheme, which focuses more on technical controls and cyber hygiene.[39] EC suppliers must also follow this scheme. Local electoral authorities are responsible for managing the risk associated with their electoral registers and voting and counting processes. They are members of the Cyber Info Sharing Partnership, a joint government–industry partnership for sharing threat intelligence.

Box 3.10 ISO/IEC 27000 and other security certifications

Recommendation EMBs should consider obtaining external certification of security-critical elements of election infrastructure to build public trust.

Building and running secure systems

It is critical for EMBs to ensure appropriate **testing, piloting and auditing** of new technologies when they are deployed in elections.

The European Union's Network and Information Security (NIS) Cooperation Group has recommended[40] that **security tests** of election systems' cybersecurity include the following:

- **Systems security testing**: Ensuring an independent review team cannot cause election systems to act in unwanted ways, using techniques such as searching for known vulnerabilities in underlying software, looking for common programming mistakes and random or 'fuzz' testing.
- **Penetration testing**: A so-called 'red team' attempts to compromise the security of deployed election systems using creative approaches by highly technically skilled testers (sometimes recruited from former hackers), reporting the results to the EMB.
- **Public testing**: A wide range of experts are invited to try and find flaws in election systems, via 'hackathons' or offering 'bug bounty' prizes to anyone that can find security vulnerabilities. This is appropriate for EMBs with mature cybersecurity policies and already well-tested systems.
- **Application code audit**: EMBs and their cybersecurity partners require auditing for vulnerabilities of the source code of applications they procure from third-party suppliers, including open source software.
- **Exercise**s: Full election attack simulations, involving senior technical and policy-making officials, will enable the most realistic test of EMB preparedness, but are expensive and time-consuming, and so most useful where there are significant concerns about forthcoming elections. Non-technical table-top exercises can be used more routinely by policy-makers. In either case, EMBs should consider involving key partner agencies and, where appropriate, private sector service providers.

The EU Network and Information Security (NIS) Cooperation Group suggests the following objectives for election cybersecurity exercises:[41]

- 'to grasp the complexities of crisis management and how to overcome the crisis;
- to understand the implications of losing trust in an IT/communication system;
- to understand the implications of an election process being compromised by an adversary;
- to test existing processes and crisis procedures for possible incidents connected with the election process;
- to point out weaknesses in existing procedures;
- to simply allow all stakeholders to become acquainted with each other, to learn names and exchange contact details.'

Box 3.11 NIS election exercise objectives

Recommendation 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.

Monitoring: Particularly for security-critical elements such as electoral rolls, and more broadly during campaigning and election periods, EMBs and their cybersecurity partners should be conducting detailed monitoring of logs, alerts and unusual network traffic within election systems and infrastructure. By earlier creating baseline profiles for equipment, anomalous behaviour can be more easily identified and investigated. This should include logs from operating systems, antivirus and firewall software, and election software; and alerts from network routers, switches and servers. Security alerts from third parties, such as IP blacklists and threat intelligence providers, can be incorporated into this monitoring.[42] Free software such as TheHive is available to support this.[43]

Recommendation 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.

A comprehensive approach: Those looking to breach the cybersecurity of an electoral process have many different opportunities, given all the various technologies used throughout the whole electoral cycle. EMBs and their cybersecurity partners need to model all of these potential avenues of attack, and ensure the risk of each is appropriately managed – as demonstrated in the South African approach in Box 3.12.

South Africa's Electoral Commission has identified the following nine principles for its comprehensive approach to security:

1. Focus is defensive – Both proactive and defensive monitoring
2. Security in depth – multi-layered segmented networks and subnets
3. Security-driven application design and development frameworks
4. User account management and access control
5. Filtering of all traffic – malware, worms, viruses, spyware, etc.
6. Continuous security monitoring of all elements
7. User access is based on a need to know
8. Continuous monitoring – Knowing when security is breached
9. Transparency – Stakeholder engagement and data sharing

Source: South Africa Electoral Commission. Box 3.12 South Africa's strategic security focus

3.4 Privacy and data protection

Electoral processes involve a significant amount of personal data, at many different stages, some of which can be highly sensitive. Its legal protection – particularly through the international consensus around data protection as an appropriate framework – is critically entwined with cybersecurity.

Some Commonwealth countries have been influenced by the 2012 Commonwealth Model Law on Data Protection,[44] and some countries (such as *Ghana*, *Mauritius* and the *UK*) have ratified the Council of Europe's Data Protection Convention. The three current and recent EU members in the Commonwealth (*Cyprus*, *Malta* and the *UK*) have implemented the EU's extensive General Data Protection Regulation.[45] Thirty-five (35) Commonwealth countries are reported to have some type of privacy or data protection law, although these vary significantly in form and function in practice.

Data protection law is a regulatory framework concerning privacy, security and data control, originating from international instruments and discussions in the mid-twentieth century (such as the OECD and Council of Europe) and inheriting aspects from various domestic laws around the world.

While the exact language different pieces of legislation use differs, it creates obligations for those who determine how data relating to individuals is used (sometimes called '*data controllers'*) and rights for the individuals (sometimes called '*data subjects'*) whom those 'personal data' concern. Data controllers require a legal basis to process data, such as consent, or a legal obligation, while data subjects can access, rectify and delete data that might identify them and is about them, as well as object to certain uses of it. Many data protection laws apply across both the public and private sectors, and there is growing consensus that almost all entities should be in scope and selectively exempted from provisions where required, rather than creating a patchy, costly and confusing set of different regimes.

Data protection is usually principle based. Data protection principles typically include fairness, lawfulness, accountability, security and limiting both the amount of data collected and how far it can be repurposed without securing a new legal basis. The principle-based nature of many (but not all) data protection regimes helps them deal with changing technologies, keeping them as *technology neutral* as possible, yet also requires a strong independent regulator to interpret these principles and a judiciary able to provide clarity on what can be technically and politically challenging issues.

Data protection legislation often also brings specific provisions designed to promote enforcement, such as the appointment of *data protection officers* inside data controllers, the mandating of *data protection impact assessments* for high-risk processing and obligatory reporting of certain categories of *data breaches* to an independent regulator.

Box 3.13 Structure and provisions of data protection law

In these and most other data protection legal frameworks, the data covered is a variant of *any information relating to an identified or identifiable individual*.[46] 'Any information' is a broad concept, which can encompass anything from a name, address, biometric data or identification number, to location data sent to a central server when using an e-voting app. Similarly, information can *relate* to individuals in many ways, such as by *content*, *purpose* or *effect* – for example, data on web browsing history locates to people by means of content, data on whether an individual has not yet voted in a political party membership election might relate by means of purpose, or information about how an individual is profiled for ad targeting might relate by means of effect.[47]

Data protection laws usually require organisations to ensure the accuracy of personal data they hold, and to correct mistakes when notified. This is a useful tool for EMBs for election-related personal data held by organisations such as political parties. Without it, EMBs may have to encourage third parties to correct data voluntarily. For example, in *Grenada*, one party app gave voters inaccurate information about their polling station location roughly 40 per cent of the time. Without a data protection law in force, the Grenada EMB had to persuade the party to fix the data.

While *identified* information is a straightforward concept, meaning information connected directly to an identifier such as a name, e-mail address or identification number, *identifiable*

information significantly widens the scope of the term.[48] It is usually considered with a balancing test, examining how far the content of the information itself, potentially in combination with other datasets in existence, could single out an individual. For example, a dataset of campaigning activity or spend, even if not attached to a candidate, could single them out through cross-referencing it to a dataset such a social media activity. In some countries, such as the *United States*, the term 'personally identifiable information' often excludes this type of data, covering only data tagged with a name or other explicit identifier. Under most *data protection* laws, as well as privacy laws in countries such as *Canada*, the term is used more broadly.

In electoral contexts, personal data relating to a range of types of individuals is likely to be processed by many different actors. These are likely to include, at least:

- Political parties or campaigns
  - Data collected during canvassing:
    - in person, including that held by volunteers;
    - remotely, such as on the telephone.
  - Data on voters and households:
    - statutorily provided electoral roll data;
    - data obtained from third parties, such as data brokers.
  - Data on party or campaign members:
    - data required for membership, such as fees;
    - political activity, such as posts held.
  - Data on staff and volunteers:
    - personal details, such as that held by human resources;
    - data on performance or tasks undertaken.
  - Data from online engagement, such as mailing lists or apps.
  - Data on competing candidates, parties and campaigns.
  - Internal communications data (e.g. between members, candidates).
- **Elected representatives** may have data beyond that of an affiliated party or campaign:
  - data from duties relating to constituents;
  - statutorily provided electoral roll data in capacity as candidate.
- Electoral management bodies:
  - staff;
  - volunteers;
  - observers;
  - data from linked bodies, such as national identity data for verification or de-duplication of electoral rolls;
  - personal data of candidates;
  - electoral roll data.
- **Journalists** are likely to have journalistic material on a range of individuals.
- **Observers** will also hold a range of data associated with their tasks.

The extensive array of this data, and the manner in which it spans sectors, actors and even jurisdictions, requires a strong and predictable legal framework. When considering electoral integrity within the context of a broader data ecosystem, which includes platforms and communications, parties, data brokers, observers, journalists and individual campaigners, sectoral laws are patchy and create significant loopholes.

Political exemptions

Data protection law often provides higher protection for 'sensitive' or 'special category' data commonly used in electoral processes, such as **data revealing political opinions or affiliations**, or **biometric data** for the purposes of identification that might be used in electronic voting systems.[49]

'Special category' or 'sensitive' data restrictions tend to have exemptions for electoral processes, but these exemptions must be balanced against the need for high protection, risk assessment and scrutiny, rather than giving a free pass to use data in ways which might be insecure or inappropriate. A report commissioned by the *UK* Information Commissioner's Office concluded:

> To the extent that contemporary elections are 'data-driven', their worst effects have been apparent in countries whose data protection laws do not cover political parties.
>
> In most democratic countries where parties are covered by data protection law, and have been for decades, there is little evidence that these restrictions have impeded their ability to perform their basic democratic roles of political mobilization, elite recruitment and policy development.[50]

Depending on the local data protection or privacy regime, some organisations involved in elections may be allowed to process these specific categories of data with lower restrictions than other actors, or even be out of scope of the law entirely. In the *United Kingdom,* for example, political parties are bound by the requirements of the Data Protection Act 2018, although registered parties benefit from being able to process data on political opinions without relying on consent (with voters allowed to opt out in writing from processing by specific parties and campaigns).[51] A similar framework can be seen in *South Africa*'s Protection of Personal Information Act 2013, although the relevant law had not yet been commenced at the time of writing.[52]

In *Malta*, the Office of the Data Protection Commissioner has stated that political parties must get consent before processing political opinions.[53] In *Australia*, political parties are not considered as organisations for the purposes of privacy law,[54] and other organisations undertaking political activities, such as parties' (sub-)contractors and volunteers, are also exempted.[55] In *Canada*, political parties 'fall between the cracks' of the national privacy regime,[56] as they are not governmental institutions for the purposes of public sector privacy law,[57] and are exempted from federal private sector privacy legislation by virtue of not meeting the definition of 'federal work, undertaking or business'.[58] Some issues around the use of the electoral roll are regulated by electoral law; however, the application and scope of this is inconsistent and patchy.[59]

Some Commonwealth countries are still developing national data protection law; the Commonwealth *Model Bill on the Protection of Personal Information* provides guidance on this, although it does not recommend derogations for political parties or purposes. This is an area of active consideration in the current update of the model law.

Recommendation Exemptions or lower restrictions for data processing in data protection and privacy laws for political organisations or purposes must be narrow and proportionate.

When organisations – whether EMBs, political parties or others – are planning to process sensitive data, they can manage the associated risks using data protection impact assessments (DPIAs) – mandated by the EU General Data Protection Regulation (GDPR)[60] for processing that is 'likely to result in a high risk to the rights and freedoms of natural persons' (§35(1)). Such assessments must contain at a minimum:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects…; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The GDPR also recommends that those affected by sensitive data processing be consulted, as well as the national data protection authority when the assessment indicates a high risk (§§35(9) and 36(1)).

In addition to data protection law, many Commonwealth countries have related provisions that focus on **unsolicited and direct marketing**. These fall in different types of law depending on the jurisdiction. In the Commonwealth's current and recent EU members (*United Kingdom*, *Cyprus* and *Malta***)**, these follow the EU ePrivacy Directive,[61] which in large

part focuses on implementing the fundamental right to confidentiality of communication.[62] In *Canada*, this issue became significantly controversial with the illegal impersonation of the EMB in the 2011 elections by a campaigner for a major party using automated calling (see Box 2.3 earlier). *South Africa*'s Electoral Commission was at the time of writing in discussions with the national Information Commissioner about protection of electoral data, with public concerns expressed about commercial marketers and debt collectors accessing voter records. In terms of the provisions of the Electoral Act, political parties have access to the full voter list (including addresses) to campaign and verify voters.

Privacy and data protection legislation is a key component of electoral integrity and cybersecurity in a complex ecosystem of data sharing and brokerage. Significant damage to perceived electoral integrity can be done if a party, campaign or candidate misuses data to manipulate voters.

Recommendation 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.

Recommendation States without a data protection or privacy law should look to enact one in line with existing international standards and institutional practices.

Personal data and privacy issues around elections should be overseen by a regulator that is truly independent from government, and which has powers and resources effective for and commensurate with its role.

Recommendation The data protection and/or privacy regulator with competence for political and electoral issues must be independent from government and adequately resourced and empowered.

Many issues around elections, such as the use of data on social media platforms or in the advertising technology domain, span borders and jurisdictions. They cannot be tackled on the domestic level alone. Regulators must therefore be part of global and regional groupings to share information and build a coherent strategy for international challenges.

Recommendation National data protection and/or privacy regulator(s) should participate in international groupings and fora to tackle international issues relating to the governance of personal data in elections.

3.5 Electoral campaigns, interference and disinformation

Digital political campaigning began in the 1990s as the World Wide Web popularised the internet outside universities, with *Canada* and *Singapore* the first Commonwealth countries to deploy broadband at scale to the general public. Commonwealth countries have seen a huge growth in broadband internet coverage, with the deployment of high-speed mobile networks and smartphone ownership in the past decade further impacting political and electoral information. While 'loose talk' is as old as civilisation itself, there is evidence that publication of falsehoods has increased due to the properties of the internet.[63]

Political rumours and misinformation were part and parcel of Nigerian politics prior to the advent of social media. For many political leaders, WhatsApp simply represents a further stage of a transformation in political communications that has gone from newspapers to radio, television, block text messages and internet-based forms of communication over the last eighty years.[64]

Election media coverage is a complex multiagency issue to regulate. Existing political coverage rules (for instance, requirements of impartiality and declarations of spending and origin of advertising) often only apply to political parties and the use of broadcast media, not

print (newspapers), online or outdoor posters. Broadcast rules can apply to all broadcasting political coverage, with a 'fairness rule' and hate speech laws and with specific regulation of electoral periods for public service broadcasters. For the 2019 general election, *India*'s Election Commission extended bans on political advertising in the 48-hour period before voting in each state from traditional media to social media.[65] The Kofi Annan Foundation has recommended that public authorities should:

- Define in law what is considered to be a political advertisement;
- Compel social media platforms to make public all information involved in the purchase of an ad, including the real identity of advertiser, amount spent, targeting criteria, and actual ad creative;
- Specify by law the minimum audience segment size for an ad; and
- Legislate a cooling-off period for digital political ads at least 48 hours before an election.[66]

Education and public trust building are vital for the conduct of all elections, particularly to communicate any changes in process or the use of technology. In Ghana, the Electoral Commission has a statutory commitment to educate people on the electoral process and its purpose. It is currently still reliant on TV, radio and flyering for communications to do so, but the new commission is keen to make improvements. It has started to use a Facebook page to communicate with voters and stakeholders, which has amassed more than 210,000 followers. It reported that it used technology to inform voters where they could access their polling stations in 2012, but not 2016. An Afrobarometer survey recently showed that significant numbers of people in Ghana rely on radio for their news and political information and that internet diffusion is less important. Social media is growing, but device cost and data pricing can still be prohibitively high, especially for people in rural areas

Box 3.14 Ghana's approach to voter education

The increase in political advertising and content production both inside and outside electoral periods in online media is capable of causing disruption to existing electoral campaign rules, with so-called 'troll factories' producing large volumes of often distorted or untrue posts which cannot be easily traced to any single source in domestic politics. The algorithms used to select which adverts are shown to social media users often promote adverts that users are more likely to click on – favouring emotional and partisan appeals even at a lower bidding price by advertisers (although in the *USA*, Facebook has disputed claims from the Trump 2016 presidential campaign its advertising costs were consequently much lower than Hillary Clinton's).[67]

Group messaging tools such as WhatsApp have been used to spread electoral disinformation in countries including *Nigeria*,[68] *Brazil*[69] and the *UK* (see Figure 3.6) – but also in Nigeria to counter it, with a study finding the app 'levels the playing field between the ruling party and the opposition and can be used to boost electoral transparency and accountability'.[70]

Figure 3.6 UK Member of Parliament warns of electoral disinformation spreading via WhatsApp during the 2019 general election

The sheer volume of social media posts has led many governments to adopt rules such as codes of conduct for the social media platforms on which posts, videos and other content is shared, rather than quixotically chasing the numerous and often anonymous posters themselves.[71]

All the respondent Commonwealth countries have experienced the online dissemination of disinformation in relation to their elections processes. Figure 3.7 shows a breakdown of the amount of reported cases per social media platform. We use disinformation to mean 'false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit',[72] and misinformation to mean unintentionally false or inaccurate information.[73] One broad challenge to regulating the intersection of modern campaigning, electoral integrity and cybersecurity is the varying abilities of EMBs to monitor the online and platform environment.

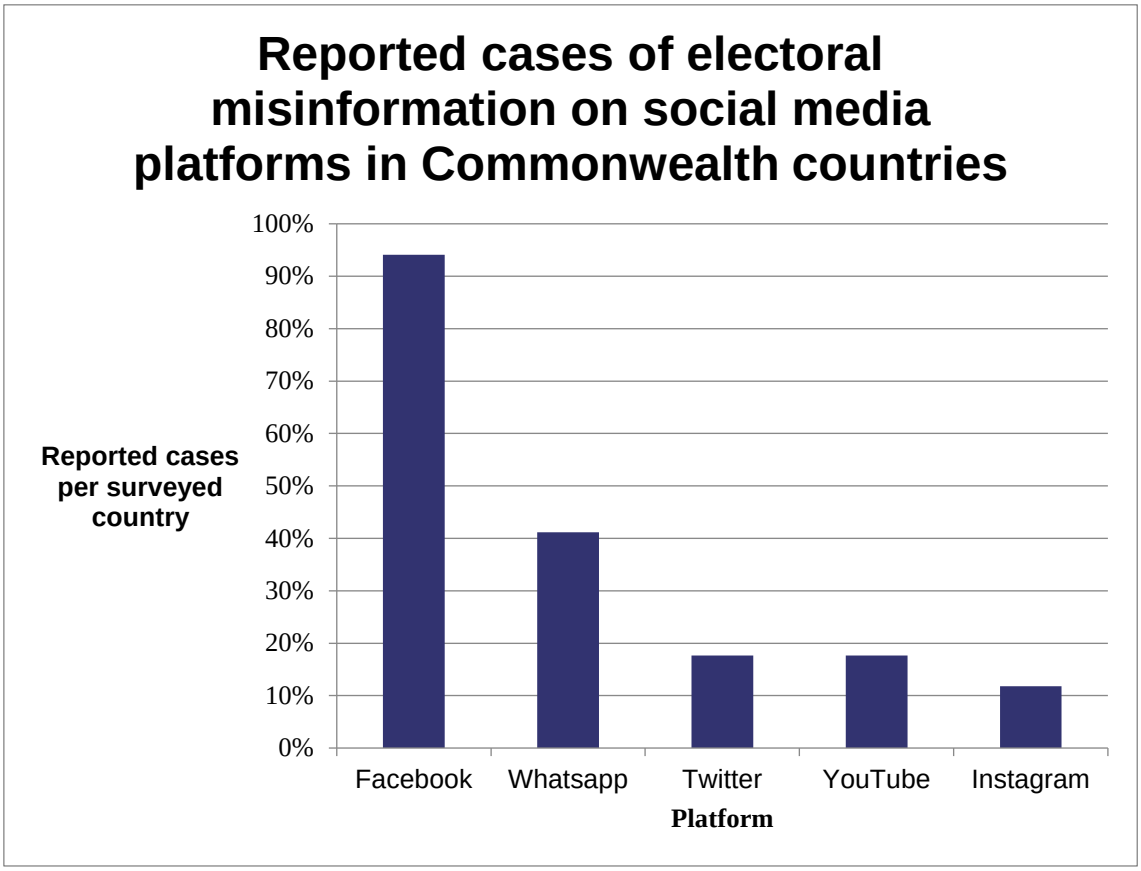


Figure 3.7 Reported cases of electoral misinformation on social media platforms in respondent Commonwealth countries

The straightforward EMB response for high-profile disinformation relating to elections is to rapidly publicise corrections, using EMB websites and social media channels, as well as interviews on broadcast media and briefings for journalists. An example of such a correction is shown in Box 3.14, from the Electoral Commission of *Ghana*. EMBs can also report clear instances of disinformation relating to elections – such as false information about the polling date or location of polling stations – to social media platforms, which will remove it where it breaches their terms and conditions.

In our discussions with Facebook's growing elections team, the company encouraged EMBs to build a relationship with them to facilitate such reporting, as well as to ensure Facebook is aware of national restrictions such as bans on political adverts close to elections or foreign political advertising. The company is also able to work with EMBs to take down fake accounts, support third-party fact checking, promote official EMB information relating to elections and provide free training for EMB staff.

Figure 3.8 Twitter warns against use of its services to manipulate or interfere in elections

In *India*, political parties must get approval for adverts from a committee organised by the EMB, which provides a QR code that must be included in an approved advert and which is checked by online platforms. The committee checks the advert content and that the publisher is certified, and also logs the price paid for the advert, which is made publicly available. Politicians must follow a code of conduct, while the EMB maintains a public website listing actions taken against violators. A 150-person Electronic Media Monitoring Committee monitors media articles during elections and transmits specific articles to districts to check. An EMB app also allows citizens to report code of conduct violations, with a photo and location; districts must deal with these reports within 100 minutes. Platforms are required to take down illegal content notified to them within 15 minutes.

Penplusbytes, which promotes citizen participation in governance and the use of ICT, worked with partners the Georgia Institute of Technology and the UN University Institute on Computing and Society during the 2016 Ghana elections to operate a Social Media Tracking Centre. Over a 72-hour pre-election period, the software monitored real-time reports over major social media platforms, directing examples of disinformation and electoral security incidents to the Electoral Commission and the National Elections Security Taskforce for action. During its deployment, the software generated 297,600 election-relevant reports (of which 183 were unique), mostly related to polling logistics such as missing ballot papers, delayed voting and failures in biometric devices. Penplusbytes reported that it detected 18 false incidents of violence, misconduct and fraud.[74]

Box 3.15 Social media tracking centre during 2016 Ghana elections

The next section focuses on two areas of growing disinformation concern where we can identify both good practices, as well as practices that seem at odds with policy objectives and, in some cases, human rights. These focus areas are closely related to cybersecurity and electoral integrity, understood broadly as a multiagency problem. The two areas are:

1. The 'switching off' of social media platforms or even blocking of the entire media by telecoms companies under order from governing parties choosing to remove social media from campaigns.
2. The use of social media to target voters, notably by disinformation intended to demotivate or even entirely mislead voters as to the electoral registration process. Examples have been interpreted by NATO as forms of foreign cybersecurity threat.

Internet 'switch-off' and disinformation laws

Internet shutdowns (general removal of transit, so that all services including e-mail are restricted by telecoms companies by order of the government) have been resorted to by

governments in the immediate election and vote counting period.[75] There have been more than 300 reported incidents of full and partial closure since 2016.[76]

In Venezuela's 2012 presidential election, Hugo 'Chávez won but died five months later of cancer, triggering an emergency election, won by Nicolás Maduro. The day before Maduro claimed victory, ['hacker for hire' Andrés] Sepúlveda hacked his Twitter account and posted allegations of election fraud. Blaming 'conspiracy hackings from abroad', the government of Venezuela disabled the Internet across the entire country for 20 minutes.[77]

Fuller reports '[i]n *Zimbabwe*, following sporadic internet blackouts in the midst of civilian protests in January 2019, the country's High Court issued a ruling in which it declared the shutdown illegal and ordered telecom operators to restore access'.[78] Purdon, Ahraf and Wagner found that '*Pakistan* has often instructed telecommunication operators to suspend mobile and/or internet networks where intelligence indicates a threat to national security'.[79] In November 2016, the African Commission on Human and Peoples' Rights noted 'the emerging practice of State Parties of interrupting or limiting access to telecommunications services such as the internet, social media and messaging services, increasingly during elections'.[80]

General internet shutdowns are contrary to international standards. UN Human Rights Council Resolution A/HRC/RES/32/13

> condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures.

A 2015 Joint Declaration by global and regional human rights bodies stated internet 'kill switches' can never be justified under international human rights law, even in times of conflict.[81] And even countries that have legislated such powers have faced constitutional law challenges, with the *Indian* Supreme Court in 2020 declaring:

> the right to freedom of speech and expression … and the right to carry on any trade or business … using the medium of internet is constitutionally protected… we think it necessary to reiterate that complete broad suspension of telecom services, be it the internet or otherwise, being a drastic measure, must be considered by the State only if 'necessary' and 'unavoidable'. In furtherance of the same, the State must assess the existence of an alternate less intrusive remedy.[82]

Recommendation 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.

Colonial-era criminal defamation laws were used in the period before the Commonwealth in response to claimed hate speech and to prevent opposition to colonial government. These have continued in many Commonwealth jurisdictions. However, in 2019, several countries passed anti-disinformation and hate speech laws for online media, extending controls into the internet environment. *Singapore* recently passed the Protection from Online Falsehoods and Manipulation Act 2019, discussed in Box 3.16.

International Grand Committee member *Singapore* in May 2019 passed a new law, the Protection from Online Falsehoods and Manipulation Act (POFMA) 2019.[83] It gives ministers powers to command online actors to remove disinformation, and regulators to stop access to internet providers in Singapore that continue to carry such messages. Part 2 of POFMA criminalises the communication of false statements of fact in Singapore in certain circumstances, and acts which enable or facilitate the communication. Section 7 provides that a person must not do any act in or outside Singapore in order to communicate in Singapore a statement knowing or having reason to believe that it is a false statement of fact that may affect political stability. Individuals who contravene section 7(1) face a fine of up to S$50,000 and/or imprisonment for up to five years. Organisations face a fine of up to $500,000. The punishment is enhanced if an unauthentic online account or a bot is used to

communicate the statement and for the purpose of accelerating the communication. Under Part 3, 'the Minister may direct the Infocomm Media Development Authority of Singapore (IMDA) to order an internet access service provider (ISP) to take reasonable steps to disable local access to the online location where the false statement of fact is communicated'.[84]

Box 3.16 Singapore's Protection from Online Falsehoods and Manipulation Act 2019

In the context of recent laws, it is important to consider their impacts in a framework of freedom of expression and human rights more generally. A joint declaration from the freedom of expression rapporteurs of several international organisations, in collaboration with international civil society groups, called for the abolition of criminal defamation laws and the wholesale avoidance of general prohibitions on disinformation.[85] The UN Human Rights Committee, established by the International Covenant on Civil and Political Rights, emphasises in General Comment No. 34 that restrictions on speech online must be strictly necessary and proportionate to achieve a legitimate purpose. The 2017 Joint Declaration by global and regional human rights bodies notes the existence of:

> attempts by some governments to suppress dissent and to control public communications through such measures as:
>
> - repressive rules regarding the establishment and operation of media outlets and/or websites;
> - interference in the operations of public and private media outlets, including by denying accreditation to their journalists and politically motivated prosecutions of journalists;
> - unduly restrictive laws on what content may not be disseminated;
> - the arbitrary imposition of states of emergency;
> - technical controls over digital technologies such as blocking, filtering, jamming and closing down digital spaces; and
> - efforts to 'privatise' control measures by pressuring intermediaries to take action to restrict content.[86]

Responses that seek to generally censor the internet or even shut it down during elections may be disproportionate, as well as illegal under international law. The Commonwealth has already concluded that direct government regulation is seen as censorship and is not the best practice answer to potential social media disinformation.[87] The Government of *Kenya* announced in the run-up to the 2017 election: 'It is not our expectation the country will be in the position to shut down internet services. We are a digital country and that is not our intention. It is not even a remote fall-back position'.[88]

Much more effective practice in democratic elections is ensuring that EMBs can liaise with social media platforms to remove and counter deliberate disinformation regarding electoral registration and voting, ensuring that claims about disinformation that form hate speech, defamation or fraud are promptly dealt with by the independent judiciary. Political name-calling can be classified by political opponents as disinformation or hate speech, which is one reason for the continued role of the independent judiciary as the arbiter of such decisions. Suspending social media platforms during elections can potentially impact large numbers of voters, whose wider communication could be jeopardised by such a restriction (for instance, suspending WhatsApp or Skype, which are vital communications tools for users).

Recommendation 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).

Regulating the use of social media to target voters

Many proposed approaches to tackling disinformation issues surround the extension of broadcast rules to non-broadcast content, whether text based or in any case at the user's individual choice. Yet care must be taken here, as this would, in all likelihood, increase the concentration of online communication in the hands of the largest platforms that can employ economies of scale in deploying proprietary filters to remove harmful content. Google, Facebook and Twitter have deployed artificial intelligence (AI) at large scale to combat disinformation, claiming this is the only cost-effective response to the billions of messages passed across their platforms daily.[89]

Opinions are divided over whether regulating such platforms is a legitimate point of intervention, in particular because this could lead to two types of content moderation 'arms race':

- in reporting disinformation, where trolls are as likely to overwhelm well-meaning citizens when each reports against the other; and
- in coding debates, so that fact checkers and other self-regulatory enforcers cannot control the amount of disinformation as it emerges in images and videos as well as text.

Examples of these content moderation arms races from the internet's regulatory history include the attempts to prevent child abuse image and terrorist video distribution, as well as unauthorised sharing of copyrighted files. In each case, the use of technologies (such as comparing hash values) in theory permitted removal before publication by the platforms deploying the technology, specifically YouTube and Facebook. In practice, the proliferation of content was restricted, but by no means prevented, by such technological intervention.

Canada: Canada has focused on traceability of political advertising, to ensure transparency in the advertising spend by major parties and to prevent violations of campaign finance laws by 'shadow' advertising by groups closely associated with political causes or parties. In Canada, it has been reported that '[t]he pre-writ period leading up to the October 21 [2019] election begins June 30; starting then, online platforms that accept political advertising in Canada will be required to show more transparency than they have in the past. Under clauses inserted in the legislation by the Commons procedure and House affairs committee and adopted by Parliament, online platforms that accept political advertising by political parties, candidates or interest groups will have to set up special ad registries that include copies of the ads and the name of the person who authorized them'.[90] While Facebook and Twitter complied with these rules, Google chose instead to prohibit Canadian political advertising.[91]

India: The Election Commission of India ('ECI') convened a meeting with representatives of social media platforms and the Internet and Mobile Association of India (IAMAI) preceding the May 2019 general elections. Social media platforms submitted a 'Voluntary Code of Ethics for the 2019 General Election'.[92] Platforms voluntarily undertook to create a dedicated reporting mechanism for the ECI, create fast response teams to take action on reported violations and facilitate political advertisement transparency. The mechanism allows ECI to notify platforms of violations under S.126, Representation of the People Act 1951. In the event of conflict between the Voluntary Code of Ethics and legal framework, the latter prevails. Platforms must take down reported content within three hours, during the two-day non-campaigning 'silence period' before polling. Platforms provide reports to IAMAI and ECI on their actions.

South Africa: Disinformation during elections is regulated by Section 89(2)(c) of the Electoral Act and Item 9(1)(b) of the Electoral Code of Conduct, which prohibits a false statement of fact, and not the expression of comments and ideas. These issues were tested in the Constitutional Court in a case concerning a text message sent by a political party to 1.5 million citizens in 2014, concerning allegations of corruption about then-President Zuma.[93] The text was found to be permitted electoral communication and not prohibited by Section 89(2). There was also a defamation offence, which has led to recent jurisprudence requiring removal of false online content.[94]

South Africa's EMB noted in 2016 the growth of online disinformation. The Directorate of Electoral Offences was established ahead of the 2016 municipal elections to investigate alleged breaches of the Electoral Code of Conduct and prohibited conduct. To help distinguish between official and fake adverts, political parties contesting the May 2019 elections were asked to upload all official advertising material used by the party to an online political advert repository at www.padre.org.za. Complaints relating to alleged breaches of the Code of Conduct must be submitted to the Electoral Court or the Directorate for Electoral Offences. In August 2019, the number of complaints and the

success rate in examination were not evaluated. In addition, the Electoral Commission launched an innovative online reporting platform for citizens to report instances of alleged digital disinformation, the 411 Campaign[95] ('411' is internet slang in southern Africa for disinformation). Developed in conjunction with Media Monitoring South Africa, the platform provided for the online submission and tracking of complaints relating to disinformation encountered on social media platforms, hosted on www.real411.org. The digital platform was intended for complaints related only to social media, and not to replace existing channels and processes for investigating alleged breaches of the Code of Conduct. By election day on 9 May 2019, 156 complaints had been logged, to be considered by a panel of relevant experts including those with expertise in media law and social and digital media.[96] They were due to make recommendations for possible further action (report awaited). Such action could include:

- referring the matter for criminal or civil legal action;
- requesting social media platforms to remove the offensive material; and/or
- issuing media statements to alert the public and correct the disinformation.

Whether these advertising registries and codes of conduct are effective in the manner described by Mozilla in Box 3.20 is yet to be seen.

Box 3.17 Social media codes of conduct and reporting in Commonwealth countries

The use of AI and machine learning to detect content has seen success in some areas, but struggles heavily in areas as value-laden, subjective and complex as disinformation.[97] Social media platforms have claimed that AI will be able to spot disinformation. But it is broadly the case that disinformation cannot be effectively automatically detected by new techniques such as machine learning, as it is highly context specific and there is no clear canonical reality against which to judge.

Automated filtering is likely to be a heavy-handed move and will result in a large number of 'false positives', where *bona fide* statements are confused with 'fake news'. Furthermore, these open up new cybersecurity threats, as machine learning systems are capable of being fooled and 'poisoned' – for example, by political actors wishing to suppress the speech of particular other voices.[98]

There is scope for standardising (the basics of) notice and appeal procedures and reporting, and creating a self-regulatory multistakeholder body, such as the UN Special Rapporteur's suggested 'social media council'.[99] Such a multistakeholder body could, on the one hand, have competence to deal with industry-wide appeals and, on the other, work towards a better understanding and minimisation of the effects of AI on freedom of expression and media pluralism.

Recommendation 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.

a. General prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.

b. Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.

c. State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).

d. State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy

information, including about matters of public interest, such as the economy, public health, security and the environment.

Box 3.18 Excerpt from the Joint Declaration on Freedom of Expression and 'Fake News'

Source: UN Special Rapporteur on Freedom of Opinion and Expression and others (2017), 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda'

Recommendation 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.

Regulatory responses and transparency requirements

The EU was the first multilateral organisation to develop a response to disinformation, investing very substantially in research and then regulation in the period since 2014.[100] The EU-orchestrated Multistakeholder Forum industry self-regulatory **Code of Practice on Online Disinformation** (see Box 3.19) was intended to demonstrate the voluntary commitments of the major social media platforms to achieve greater transparency in political advertising, prior to the European Parliament elections of May 2019.[101] This was the world's second largest democratic election after *India's* parliamentary election.

The EU Code of Practice on Disinformation includes the following commitments:

1. scrutiny of ad placements, political and 'issue-based' advertising:
    a. disrupt advertising and monetisation incentives for relevant behaviours;
    b. ensure that advertisements are clearly distinguishable from editorial content;
    c. enable public disclosure of political advertising;
    d. use reasonable efforts towards devising approaches to publicly disclose 'issue-based advertising';
2. integrity of services:
    a. put in place clear policies regarding identity and the misuse of automated bots;
    b. put in place policies on what constitutes impermissible use of automated systems and to make this policy publicly available on the platform and accessible to EU users;
3. empowering users:
    a. help people make informed decisions when they encounter online news that may be false, including by supporting efforts to develop and implement effective indicators of trustworthiness in collaboration with the news ecosystem;
    b. invest in technological means to prioritise relevant, authentic and authoritative information;
    c. invest in features and tools to make it easier to find diverse perspectives;
    d. support efforts aimed at improving critical thinking and digital media literacy;
    e. encourage market uptake of tools that help consumers understand why they are seeing particular advertisements;
4. empowering the research community:

a. support good faith independent efforts to track and research disinformation and political advertising, including the independent network of fact-checkers facilitated by the European Commission;

b. convene an annual event to foster discussions within academia, the fact-checking community and members of the value chain.

Box 3.19 The EU Code of Practice on Disinformation

Source: European Commission

Part of the industry response to the EU Code of Practice concerned rectifying the limited access platforms provide to political advertisements using their systems. Explicitly paid for political advertisements are increasingly placed in online 'ad archives', such as those provided by Facebook and by Google.[102] The main intention of these codes of practice and their implementation by platforms is to allow civil society actors and regulators to identify and audit the political advertising spend by actors deemed political by the platform. Users themselves can access such an archive, but the information in the archive is not currently presented to them when, for example, they browse a site and view an advert.

Twitter decided on 30 October 2019, to ban all explicit political advertising.[103] This leaves political actors to insert surreptitious political messaging and to attempt to create viral memes using both real and fake ('bot') accounts, which have been proved to be ubiquitous on social media platforms. An advertising ban in itself would only stem part of the disinformation flood on social media. Facebook's Mark Zuckerberg on 31 January 2020 explained he would explicitly permit all political advertising, whether factual or disinformation, using the US Constitution's First Amendment to justify what he describes as 'political speech'.[104] The European Commission's higher political priority for regulation opposed to Facebook's free market was explained by Vice President Jourova on 30 January 2020, stating Europe 'will also need some degree of regulation, in particular addressed to the platforms'.[105]

The Mozilla Foundation has proposed, along with more than 70 researchers, standards for effective political advertising archives that should be enforced upon platforms.[106] Their suggestions are in Box 3.20.

1. The ad archive should be comprehensive, including
    a. direct electioneering content
    b. candidates or holders of political office
    c. matters of legislation or decisions of a court
    d. functions of government
2. The ad archive should provide information about targeting criteria and information about impressions, content, payment, and microtargeting features
3. The ad archive must support research, by allowing bulk access and download and persistent, well-documented meta-data
4. The ad archive should contain both up-to-date and historical data
5. The ad archive should be accessible to the public.

Box 3.20 Mozilla Foundation recommendations on political advertising archives

A consistent challenge is ensuring that companies deliver workable advertising archives, such as those in line with the above guidelines. In the EU, Facebook's attempt to create such a system has been described as 'inadequate', pointing to challenges in enforcement more broadly.[107] Commonwealth countries that have not placed explicit requirements on platforms to provide such advertising archives in their law will face steep challenges in overseeing campaign spending online. The *UK*'s Centre for Data Ethics and Innovation has recommended

'[Social media] Platforms should be required to host publicly accessible archives for online political advertising'.[108]

Recommendation 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.

NATO has reported the continued need for EMB and wider government readiness against disinformation threats.[109] In a cybersecurity context, they point to the large and changing 'scale of the black-market infrastructure for developing and maintaining social metric manipulation software, generating fictitious accounts, and providing mobile proxies and solutions for SMS activation'.[110] These systems rely on security loopholes, data breaches and the use of bots at scale in order to influence disinformation on a large scale. Recommendations from NATO can be found in Box 3.21.

1. Monitoring of targeted, co-ordinated attempts to influence decision-making of voters, including the misuse of large interest groups, pages and other moderated forums for political purposes through automation, increased manual moderation and assessments, or new technical solutions to prevent malicious use.

2. Monitoring of impersonation of government and public accounts.

3. Ad transparency, specifically regarding the micro-targeting of segments of the public.

4. Recognition and swift elimination of the use of non-organic manipulation of user engagement in order to manipulate the perceived popularity of a certain view, or of certain content.

5. Transparency and accountability to enable greater public insight and involvement in securing the online environment.

6. User-friendly integration of fact-checking mechanisms.

Box 3.21 NATO Strategic Communications Centre of Excellence Recommendations

Recommendation 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.

Disinformation threats may seek to suppress or increase voter motivation in specific targeted segments of the population by geography or expressed political motivation – so-called micro-targeting to 'fire up the base' (motivate) or to suppress voter turnout via demotivational messages.

Recommendation 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.

Notes and references

[1] Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization* 25(8), pp.1397–1418.

[2] US National Institute of Standards and Technology (2012), *Guide for Conducting Risk Assessments*, Special Publication 800-30 Revision 1, September, p.1, available at: https://www.nist.gov/publications/guide-conducting-risk-assessments
[3] Ibid, p.6.
[4] Ibid, pp.8–12.
[5] Information Systems Audit and Control Association (ISACA) (2013), *COBIT 5 for Risk*, available at: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf
[6] J Freund and J Jones (2014), *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann (Oxford).
[7] US National Institute of Standards and Technology (2012), op. cit. endnote 2.
[8] NATO Strategic Communications Centre of Excellence (2019), *Protecting Elections: A Strategic Communications Approach*, June. NATO Stratcom Coe (Latvia).
[9] Cross-government co-ordination in electoral cybersecurity has recently been recommended by the European Commission. See: *Recommendation of the Commission on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament* (12 Sep 2018, C(2018) 5949 final).
[10] Government of the Republic of Trinidad and Tobago (2012), *National Cyber Security Strategy*, prepared by the Inter-Ministerial Committee for Cyber Security, December, available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TrinidadandTobagoNationalCyberSecurityStategyEnglish.pdf
[11] NATO Strategic Communications Centre of Excellence (2019), op. cit. endnote 8, p.12
[12] Ibid, p.18
[13] Ian Brown and James Lee (2019), Interviews with the Electoral Commission of Ghana, March.
[14] Ghana Journalist Association (GJA) (undated), 'GJA Guidelines on Election Coverage', available at: http://www.gjaghana.org/index.php/2017-02-08-22-16-14/gja-guidelines-on-election-coverage
[15] Secretary-General of the Commonwealth, Patricia Scotland (2018), 'Bringing education goals within reach', 7 February, available at: https://thecommonwealth.org/media/press-release/bringing-education-goals-within-reach
[16] Kshetri, Nir (2016), 'Cybersecurity and Development', *Markets, Globalization & Development Review*, 1(2), article 3, pp.6–7.
[17] NATO Strategic Communications Centre of Excellence (2019), op. cit. endnote 8, p.17
[18] International Institute for Democracy and Electoral Assistance, available at: https://www.idea.int/
[19] MISP is a 'threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information'. See: https://www.misp-project.org
[20] Organization of American States (2010), *Observing the Use of Electoral Technologies: A Manual for OAS Electoral Observation Missions*, OEA/Ser.D/XX, available at: https://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf
[21] Organization of American States (2019), *Electoral integrity analysis, General Elections in the Plurinational State of Bolivia, October 20, 2019: Preliminary Findings Report to the General Secretariat*, available at: http://www.oas.org/documents/eng/press/Electoral-Integrity-Analysis-Bolivia2019.pdf
[22] Alliance of Democracies, Transatlantic Commission on Elections Integrity (undated), 'Pledge for Election Integrity', available at: https://electionpledge.org
[23] Canada Communications Security Establishment (2019), *2019 Update: Cyber Threats to Canada's Democratic Process*, p.19
[24] See, for example, the regular guidance produced by the UK National Cyber Security Centre for businesses and individuals, such as the poster and free online training for businesses available at: https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
[25] See, for example, the challenge of the French National Cybersecurity Agency working with political parties without its assistance being actively sought. EU NIS Cooperation Group (2018), 'Compendium on Cyber Security of Election Technology' (03/2018), p.45.
[26] National Academies of Sciences, Engineering, and Medicine (2018), *Securing the Vote: Protecting American Democracy*, The National Academies Press, Washington, DC, pp.64–65, available at: https://doi.org/10.17226/25120
[27] D Bradbury (2013), 'India's Cybersecurity challenge', available at: https://www.infosecurity-magazine.com/magazine-features/indias-cybersecurity-challenge/
[28] National Academies of Sciences, Engineering, and Medicine (2018), op. cit. endnote 26.
[29] Australian Cyber Security Centre (2017), *Strategies to Mitigate Cyber Security Incidents*, February, available at: https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
[30] See this detailed analysis: Digital Shadows Photon Research Team (2020), *Two-Factor in Review*, January, available at: https://resources.digitalshadows.com/whitepapers-and-reports/two-factor-in-review
[31] UK National Cyber Security Centre, available at: https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html

[32] UK National Cyber Security Centre (2020), *Advice and guidance*, available at: https://www.ncsc.gov.uk/section/advice-guidance/all-topics
[33] NATO Strategic Communications Centre of Excellence (2019), op. cit. endnote 8, pp.13–15.
[34] Katherine Ellena and Goran Petrov (2018), *Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies, International Foundation for Electoral Systems*, October, p.32.
[35] An example in the neighbouring field of banking security is a US initiative to streamline regulation, where 'The intent ultimately is that all regulators, domestically and internationally, would have the same standards'. See Kiran Stacey, Laura Noonan and Robert Armstrong (2019), 'US banks face tighter scrutiny of cyber defences', *Financial Times*, 17 June, available at: https://www.ft.com/content/69a25232-8eaa-11e9-a1c1-51bf8f989972
[36] P Mell and T Grance (NIST) (2011), The NIST Definition of Cloud Computing, p.2 available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[37] Ian Brown and James Lee (2019), Commonwealth Secretariat regional training workshop for Asia Pacific EMBs on Election Cybersecurity.
[38] ISO/IEC Joint Technical Committee 1/SC 27 (2016), 'Information technology – Security techniques – Information security management systems – Overview and vocabulary'. International Organization for Standardization; Deutsches Institut für Normung, Berlin, Germany.
[39] UK National Cyber Security Centre, available at: https://www.cyberessentials.ncsc.gov.uk
[40] EU NIS Cooperation Group (2018), 'Compendium on Cyber Security of Election Technology' (03/2018), pp.27–31.
[41] Ibid, pp.30–31.
[42] Ibid, p.35.
[43] 'A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.' See: https://thehive-project.org/#section_thehive and https://thehive-project.org/#section_cortex for analysis and response tools.
[44] The Commonwealth, Office of Civil and Criminal Justice Reform (2017), *Model Bill on the Protection of Personal Information,* The Commonwealth, London.
[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p.1.
[46] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by its Protocol CETS No. 223 (opened for signature 28 January 1981, entered into force 1 October 1985) 108 ETS ('Council of Europe Convention 108') art 2(a).
[47] See, for example, the interpretation of the European Court of Justice, Case C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994 para 35.
[48] The Commonwealth Model Data Protection Law only uses 'identifiable' rather than identified. See endnote 44.
[49] See, for example, GDPR, article 9.
[50] Colin Bennett and Smith Oduro-Marfo (2019), *Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities*, University of Victoria, p.ii, available at: https://icdppc.org/wp-content/uploads/2019/10/Privacy-and-International-Democratic-Engagement_finalv2.pdf
[51] Data Protection Act 2018 (United Kingdom) sch 1 para 22.
[52] Protection of Personal Information Act 2013 (South Africa) s 31.
[53] Yannick Pace (2018), 'Parties face hefty fines over electoral profiling without consent', *MaltaToday*, 30 May.
[54] Privacy Act 1988 (Australia) s 6C(1).
[55] Privacy Act 1988 (Australia) s 7C.
[56] Colin J Bennett and Robin M Bayley (2012), *Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis,* Office of the Privacy Commissioner of Canada.
[57] Privacy Act 1982 (Canada) s 3.
[58] Personal Information Protection and Electronic Documents Act SC 2000, c. 5 (Canada) s 4(1).
[59] Bennett and Bayley (2012), op. cit. endnote 56.
[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, op. cit. endnote 45, p.1.
[61] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services; Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p.11–36.
[62] Frederik J Zuiderveen Borgesius and Wilfred Steenbruggen (2019), 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust', 20 Theoretical Inquiries in Law 291. Cegla Center for Interdisciplinary Research of the Law. Buchmann Faculty of Law, Tel Aviv University.
[63] John Suler (2004), 'The Online Disinhibition Effect', *CyberPsychology & Behavior*, 6/1/2004, Vol. 7 Issue 3, p.321.

[64] Jamie Hitchen, Idayat Hassan, Jonathan Fisher and Nic Cheeseman (2019), *WhatsApp and Nigeria's 2019 Elections: Mobilising the People, Protecting the Vote*, Centre for Democracy & Development, p.5.
[65] Neha Alawadhi and Karan Choudhury (2019), 'No political ads on social media ahead of polls?', Thank Election Commission, *Business Standard*, 11 April, available at: https://www.business-standard.com/article/elections/no-political-ads-on-social-media-ahead-of-polls-thank-election-commission-119041100055_1.html
[66] Kofi Annan Commission on Elections and Democracy in the Digital Age (2020), *Protecting Electoral Integrity in the Digital Age*, January, pp.94–95. Kofi Annan Foundation (Geneva, Switzerland).
[67] Ali Breland (2018), 'Facebook says Trump paid more than Clinton for digital advertising', *The Hill*, 27 February, available at: https://thehill.com/policy/technology/375915-facebook-says-trump-paid-more-than-clinton-for-digital-advertising
[68] Hitchen et al. (2019), op cit. endnote 64.
[69] Caio Machado, Beatriz Kira, Gustavo Hirsch, Nahema Marchal, Bence Kollanyi, Philip N Howard, Thomas Lederer and Vlad Barash (2018), 'News and Political Information Consumption in Brazil: Mapping the First Round of the 2018 Brazilian Presidential Election on Twitter', Data Memo.4, Project on Computational Propaganda, Oxford, UK.
[70] Hitchen et al. (2019), op cit. endnote 64, p.4.
[71] Ian Brown, Lilian Edward and Christopher T Marsden (2009), 'Information Security and Cybercrime', in L Edwards and C Waelde (eds.), Law and The Internet (3rd edn.), Hart, Oxford.
[72] High Level Expert Group on Fake News and Online Disinformation (2018), *Report to the European Commission on A Multi-Dimensional Approach to Disinformation*, p.10, available at: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation
[73] C Wardle and H Derakhstan (2017), *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (DGI(2017)09), Shorenstein Center on Media, Politics and Public Policy at Harvard Kennedy School for the Council of Europe, available at: https://shorensteincenter.org/information-disorder-framework-for-research-and-policymaking. The EU's interinstitutional terminology database IATE (Inter-Active Terminology for Europe) specifically notes that disinformation should not be confused with misinformation, defined in IATE as 'information which is wrong or misleading but not deliberately so'. See N Bentzen (2015), *Understanding Propaganda and Disinformation, European Parliament Research Service At a Glance*, available at: http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571332/EPRS_ATA(2015)571332_EN.pdf
[74] Penplusbytes (2017), *Ghana's Media Comes of Age in Elections Coverage*, January, available at: http://penplusbytes.org/ghanas-media-comes-of-age-in-elections-coverage/
[75] Reporters Without Borders (2019), 'Benin's citizens deprived of Internet on election day', 1 May, available at: https://rsf.org/en/news/benins-citizens-deprived-internet-election-day. Reporters Without Borders is one of 190 members of the #KeepItOn coalition against internet censorship during elections.
[76] Simon Fuller (2019), 'Our digital future', *International Bar Association Global Insight*, June/July 2019, 11 June, available at: https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=60554B04-C95A-494B-845B-60BAFC7CA4C6 reports Access Now's #KeepItOn coalition 'documented 371 shutdowns between 2016 and 2018, including 310 in Asia and 12 in Europe'.
[77] Jordan Robertson, Michael Riley and Andrew Willis (2016), 'How to Hack an Election', *Bloomberg Businessweek*, 31 March, available at: https://www.bloomberg.com/features/2016-how-to-hack-an-election/
[78] Fuller (2019), op. cit. endnote 76.
[79] Lucy Purdon, Arsalan Ashraf and Ben Wagner (2015), 'Security v Access: The Impact of Mobile Network Shutdowns, Case Study Telenor Pakistan', Internet Policy Observatory, available at: https://repository.upenn.edu/internetpolicyobservatory/13
[80] ACHPR/Res. 362 (LIX), on the right to freedom of information and expression on the internet in Africa.
[81] Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, presented at the UNESCO World Press Freedom Day event, 4 May 2015, section 4(c).
[82] *Anuradha Bhasin and others vs Union of India and others* (2020) SCC OnLine SC 1031/1164, §§28 and 99.
[83] Protection from Online Falsehoods and Manipulation Act 2019 passed 8 May 2019, available at: https://sso.agc.gov.sg/Bills-Supp/10-2019/Published/20190401?DocDate=20190401
[84] Darren Grayson Chng (2019), 'POFMA: Singapore's anti-fake news law', Society for Computers and Law, May, available at: https://www.scl.org/articles/10541-pofma-singapore-s-anti-fake-news-law
[85] In very narrow specific circumstances pertaining to judicial reputation, criminal defamation with a financial penalty rather than imprisonment has been considered appropriate in the European Court of Human Rights: *Peruzzi v Italy* (App no 39294/09) judgment of 30 June 2015.
[86] UN Special Rapporteur on Freedom of Opinion and Expression and others (2017), 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda', p.2.
[87] The Commonwealth (2016: 6): 'While there may be a tendency to seek to regulate a way out of this "problem", countries should remember that this is likely to prove difficult – and that regulation may even result in the

restriction of certain legitimate freedoms. Attempting to regulate freedom of expression, for example, can often prove counter-productive, so there is good reason for caution in this regard. Moreover, as they seek to address these challenges, countries should bear in mind that it is unlikely that legislative change will be able to keep pace with the dynamic evolution of the new media environment'.

[88] Vincent Kejitan (2017), 'Government Says There Will be No Internet Shutdown During Elections', Kenyans.co.ke, 27 June, available at: https://www.kenyans.co.ke/news/20435-government-says-there-will-be-no-internet-shutdown-during-elections

[89] C Marsden and T Meyer (2019), 'Regulating Disinformation with Artificial Intelligence (AI): The effects of disinformation initiatives on freedom of expression and media pluralism', at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

[90] Elizabeth Thompson (2019), 'Most of Canada's top websites won't post federal election ads this year: Many of the most popular sites decided it was too late to set up a registry', CBC News 1 May, available at: https://www.cbc.ca/news/politics/online-election-advertising-canada-1.5116753

[91] Alex Boutilier (2019), 'Twitter announces rules for Canadian political advertising', *The Star*, 29 August, available at: https://www.thestar.com/politics/federal/2019/08/29/twitter-announces-rules-for-canadian-political-advertising.html

[92] Press Information Bureau , Government of India (2019), 'Voluntary Code Of Ethics For The 2019 General Election', available at: https://pib.gov.in/newsite/PrintRelease.aspx?relid=189494

[93] *Democratic Alliance v African National Congress*, Case CCT 76/14, 19 January 2015, available at: https://globalfreedomofexpression.columbia.edu/cases/democratic-alliance-v-african-national-congress/ (Source: Columbia Global Freedom of Expression).

[94] *Trevor Manuel v Economic Freedom Fighters and Others* ([2019] ZAGPJHC 157) Johannesburg High Court 30 May.

[95] Electoral Commission of South Africa (2019, undated), 'Report digital disinformation', available at: https://www.elections.org.za/content/Elections/2019-National-and-provincial-elections/Report-digital-disinformation/

[96] Real 411, available at: https://www.real411.org/complaints

[97] C Marsden and T Meyer (2019), 'How can the law regulate removal of fake news?', *Computers and Law*, available at: https://www.scl.org/articles/10425-how-can-the-law-regulate-removal-of-fake-news

[98] See, generally, Battista Biggio and Fabio Roli (2018), 'Wild Patterns: Ten Years after the Rise of Adversarial Machine Learning', 84 Pattern Recognition 317.

[99] UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2018), *Report on A Human Rights Approach to Platform Content Regulation*, supra 31, paras 58, 59, 63, 72.

[100] T Meyer, C Marsden and I Brown (2020, in print), 'Regulating disinformation with technology: analysis of policy initiatives relevant to illegal content and disinformation online in the European Union', in E Kużelewska, G Terzis, D Trottier and D Kloza (eds.) *Disinformation and digital media as a challenge for democracy*, European Integration and Democracy Series, Vol. 6, Intersentia, Cambridge.

[101] EU Code of Practice on Disinformation (2018), available at: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. The 2019 election had a 50.62 per cent turnout, see: https://election-results.eu/turnout/

[102] See, for example, Facebook's 'Ad Library', available at: https://www.facebook.com/ads/library; for Google see 'Political advertising on Google', available at: https://transparencyreport.google.com/political-ads/.

[103] See Twitter (2019), 'Twitter to ban political advertising', available at: https://twitter.com/i/events/1189643849385177088

[104] Edward Helmore (2020), 'Facebook commitment to free speech will "piss people off", Zuckerberg says', *The Guardian*, Sat 1 Feb 20.03 GMT, available at: https://www.theguardian.com/technology/2020/feb/01/facebook-political-ads-zuckerberg

[105] European Commission (2020), Speech, 30 January 2020, Brussels, Opening speech of Vice-President Věra Jourová at the conference Disinfo Horizon: Responding to Future Threats, available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_20_160

[106] Mozilla (2017), 'Facebook and Google: This is What an Effective Ad Archive API Looks Like', The Mozilla Blog, 27 March, available at: https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like (accessed 21 June 2019).

[107] Mozilla, 'Facebook's Ad Archive API is Inadequate', The Mozilla Blog, 29 April 2019, available at: https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate (accessed 7 July 2019).

[108] Centre for Data Ethics and Innovation (2020), Online targeting: Final report and recommendations, February. Department for Digital, Culture, Media and Sport (London, United Kingdom).

[109] NATO Strategic Communications Centre of Excellence (2018), *The Black Market for Social Media Manipulation*, November. NATO Stratcom Coe (Latvia).

[110] Ibid.

Chapter 4 Concluding remarks

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.*[1]

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'.[2] 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'[3] – 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'.[4]

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] Nic Cheeseman and Brian Klaas (2019), *How to Rig an Election*, Yale University Press, New Haven, pp.236–237.
[2] 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
[3] Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization,* 25(8), p.1410.
[4] Ibid, p.1410.