Chapter 1

Introduction

Chapter 1
Introduction

1.1 The increasing vulnerability of electoral systems

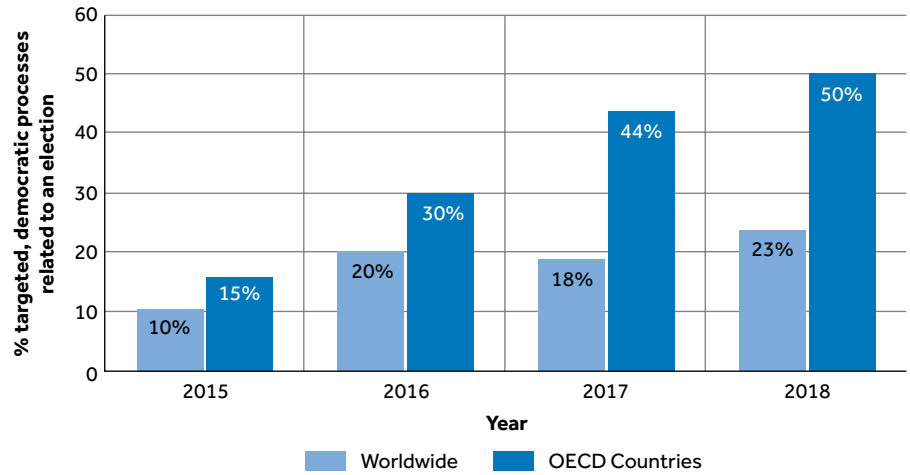
Since the 1990s, internet-connected computers, mobile and 'smart' devices have become integral parts of day-to-day life for many in the Commonwealth, including for election-related activities.

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).

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.

Figure 1.1 Threat activity targeting democratic processes observed by Government of Canada, Communications Security Establishment (CSE)



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

Table 1.1 Grouping of survey respondents

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		

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.

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 32 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.

Box 1.1 Models of interagency collaboration

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?

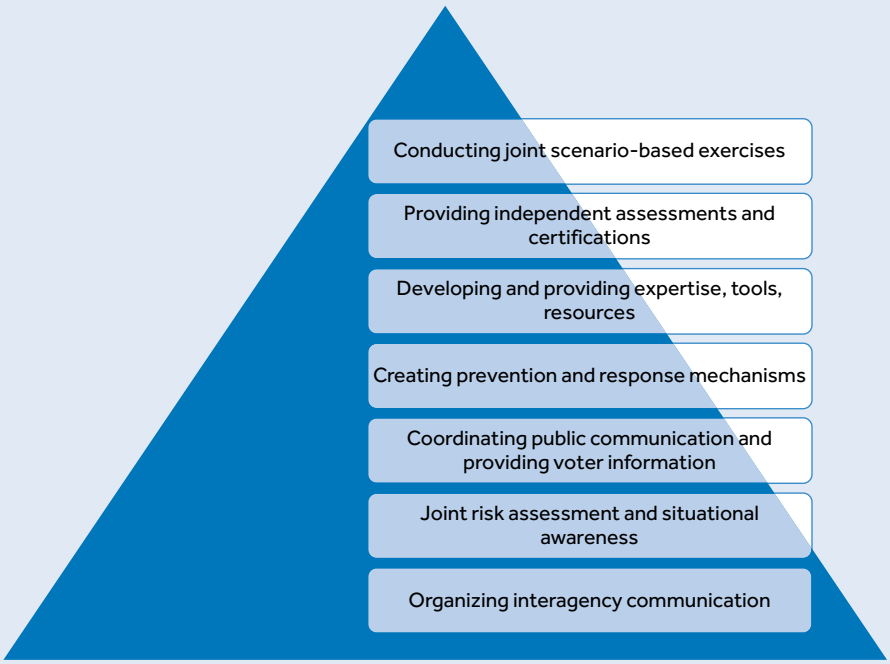
The publication finds that it is easier for centralised EMBs to implement uniform cybersecurity measures throughout the country and that those with decentralised institutions will often bear the brunt of the criticism for cyberattacks, despite not having full operational control. Decentralised EMBs therefore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

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

Figure 1.2 International IDEA's levels of multiagency collaboration



- 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.

Source: International Institute for Democracy and Electoral Assistance (IDEA)

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.

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.

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.

Public procurement law governs the way that public bodies of all types obtain digital technologies, and may place restrictions on which suppliers

Figure 1.3 Ghana's National Communications Authority advertises its anti-spam SMS service

Box 1.2 International co-operation by Ghana

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.

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.

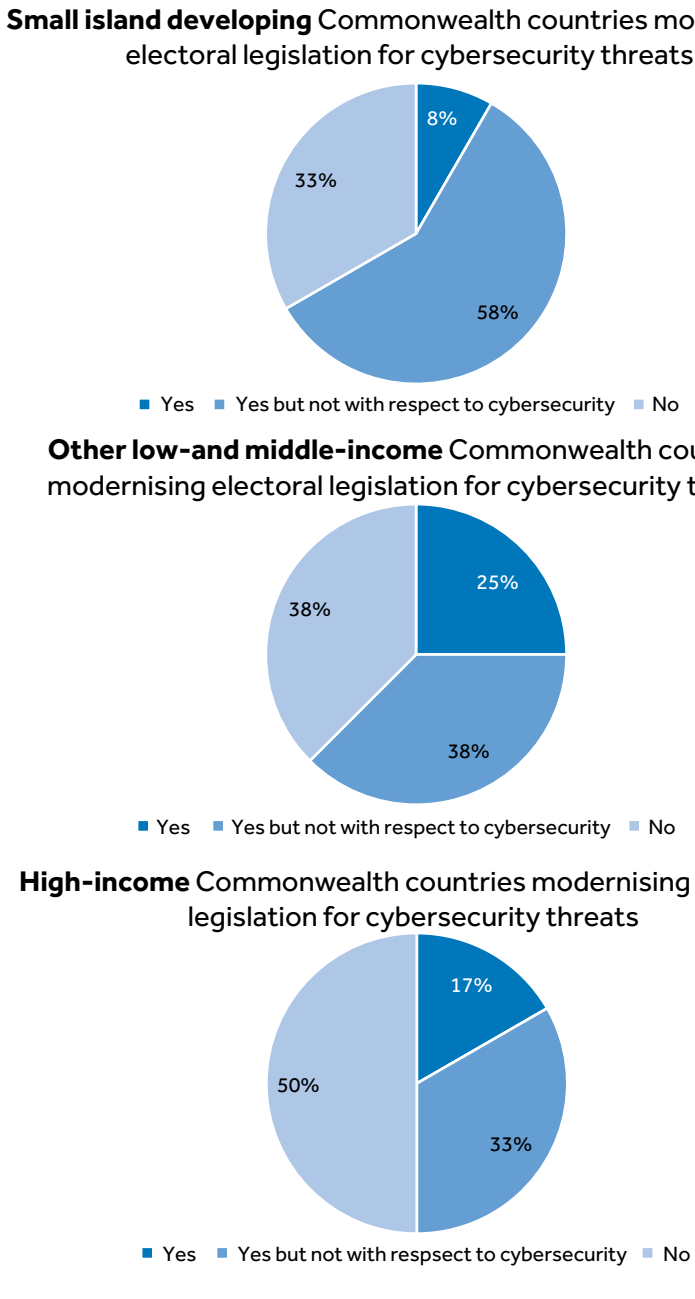
Laws concerning **freedom of expression**, which often have a constitutional foundation, are important, particularly when read alongside **broadcasting law**, **media regulation** and **defamation law**. Many of these pieces of legislation are looked to regarding deceptive content online, such as fake 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 1.4) 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]

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.

Figure 1.4 Proportion of respondent Commonwealth countries modernising electoral legislation for cybersecurity threats



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

Box 1.3 Ghana's National Cyber Security Centre

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

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.

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]

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 1.5). 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*).

Some data protection authorities have seen significant budget increases in recent years to cope with changing legislation and changing issues. The

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

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		

Source: Commonwealth Secretariat

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 Government of Canada, Communications Security Establishment (CSE) (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 unofficial 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.