Chapter 3
Overarching Best Practices for Secure Elections

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 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.

Box 3.1 Risk management tools and approaches

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

(*Continued*)

Box 3.1 Risk management tools and approaches (*Continued*)

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]

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.

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

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.

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.

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]

Box 3.3 New Zealand cross-agency working

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.

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.

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.

Box 3.4 Ghana's media environment

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]

> *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]

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

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'.

(*Continued*)

Box 3.5 OAS preliminary audit of the Bolivian presidential elections on 20 October 2019 (*Continued*)

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'.

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.

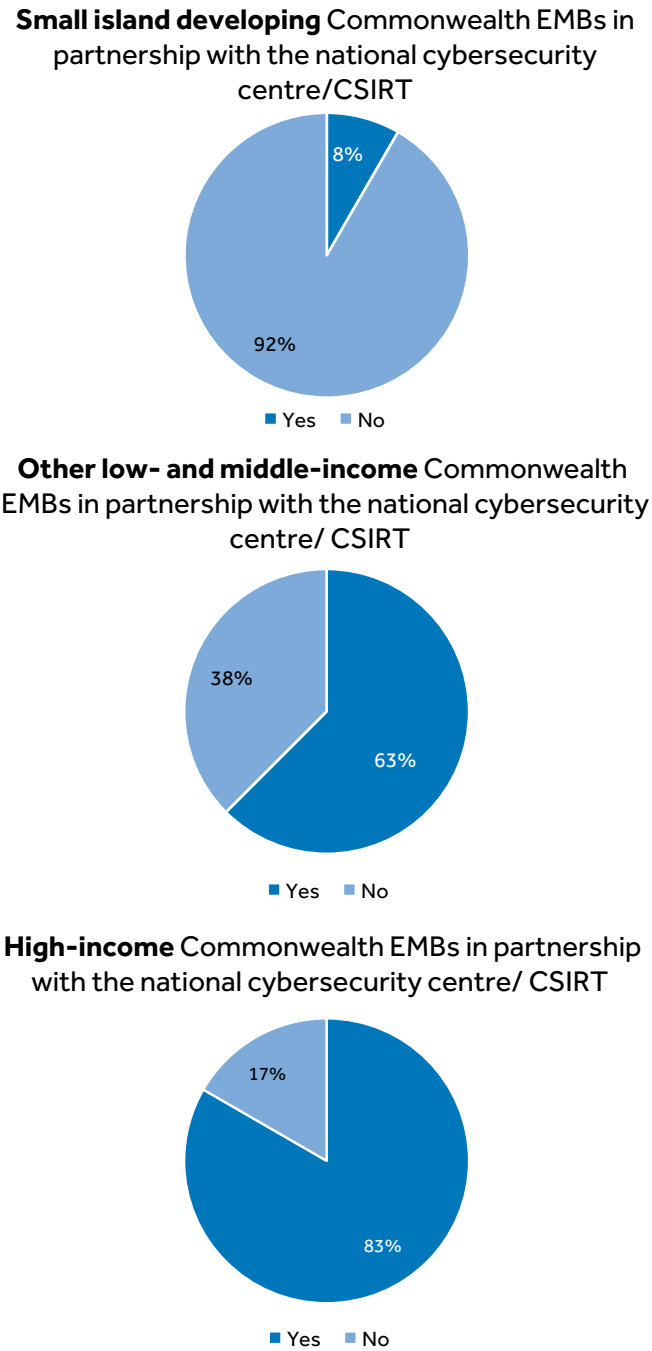
In some countries, such as *Ghana* and *Trinidad and Tobago*, these centres play a mandatory role in securing systems the government has designated as critical national infrastructure (CNI). In *India*, where election systems have been declared to be CNI, the EMB may consequently create security regulations – 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

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



the Electoral Commission's offices, but the country is looking into central integration with the government's networks.

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.

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

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

(*Continued*)

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

> 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.

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

Box 3.7 Ghana cybersecurity training initiatives

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.

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.

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

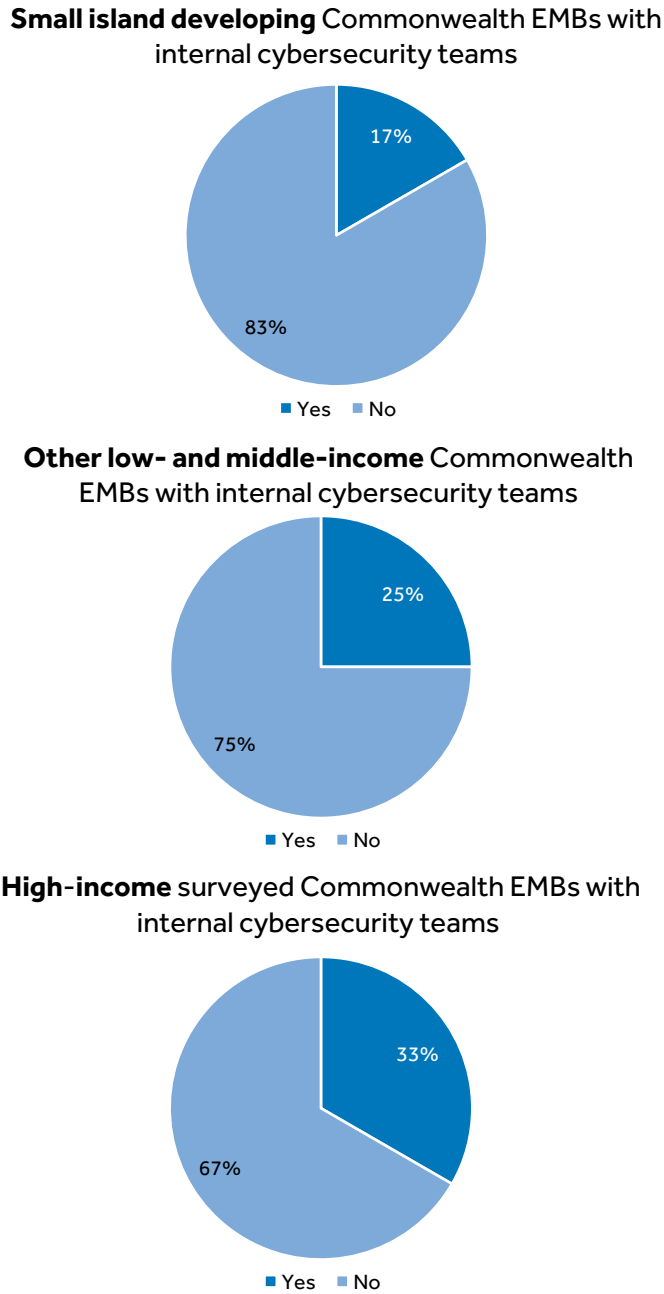
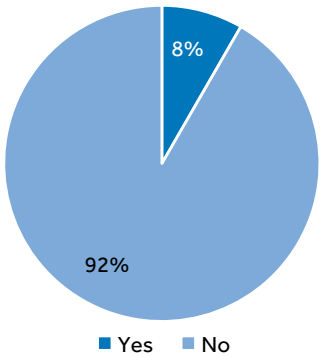
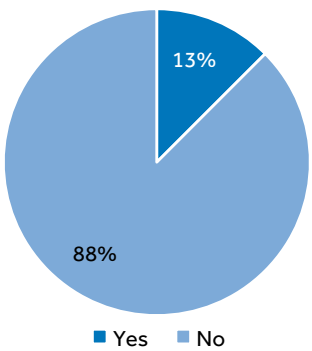


Figure 3.3 Proportion of respondent Commonwealth EMBs who have commissioner or board-level cybersecurity representation

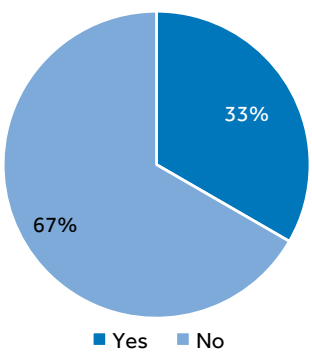
Small island developing Commonwealth EMBs with commissioner or board-level cybersecurity representation



Other low- and middle-income Commonwealth EMBs with commissioner or board-level cybersecurity representation



High-income Commonwealth EMBs with commissioner or board-level cybersecurity representation



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.

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.

Box 3.8 The UK *Cyber Essentials* scheme

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.

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]

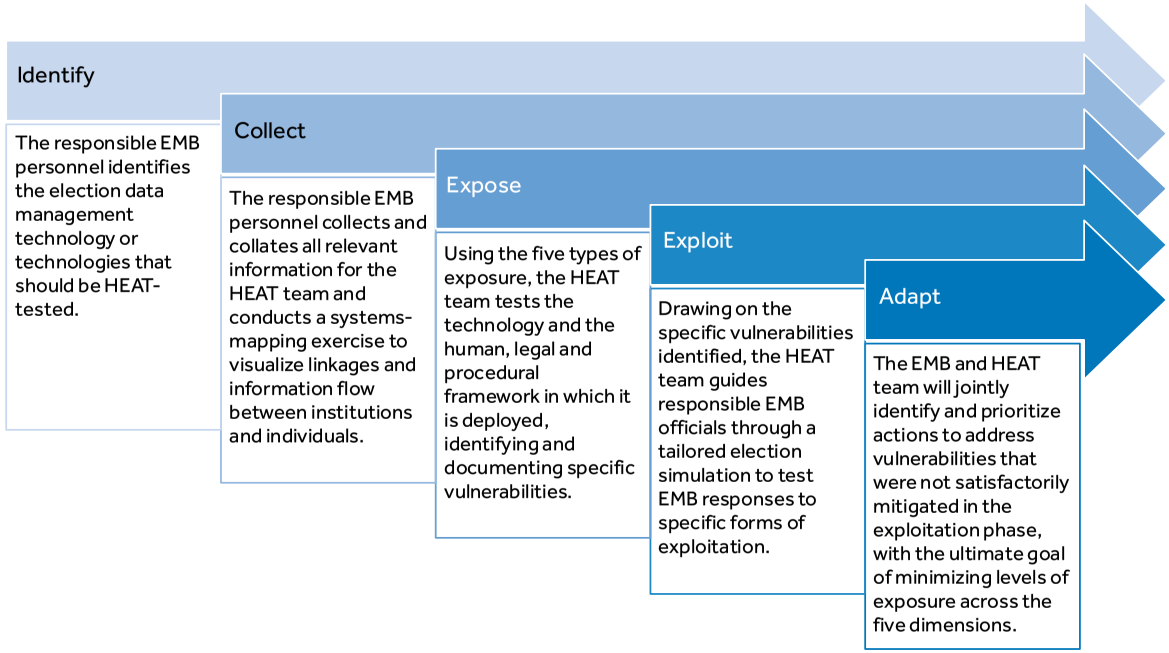
Recommendation EMBs should provide cybersecurity training for all staff, as well as career development for technical staff, partnering with local universities, regional peers and international organisations.

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.

Box 3.9 Commonwealth EMB use of cloud computing

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.

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.

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.

Box 3.10 ISO/IEC 27000 and other security certifications

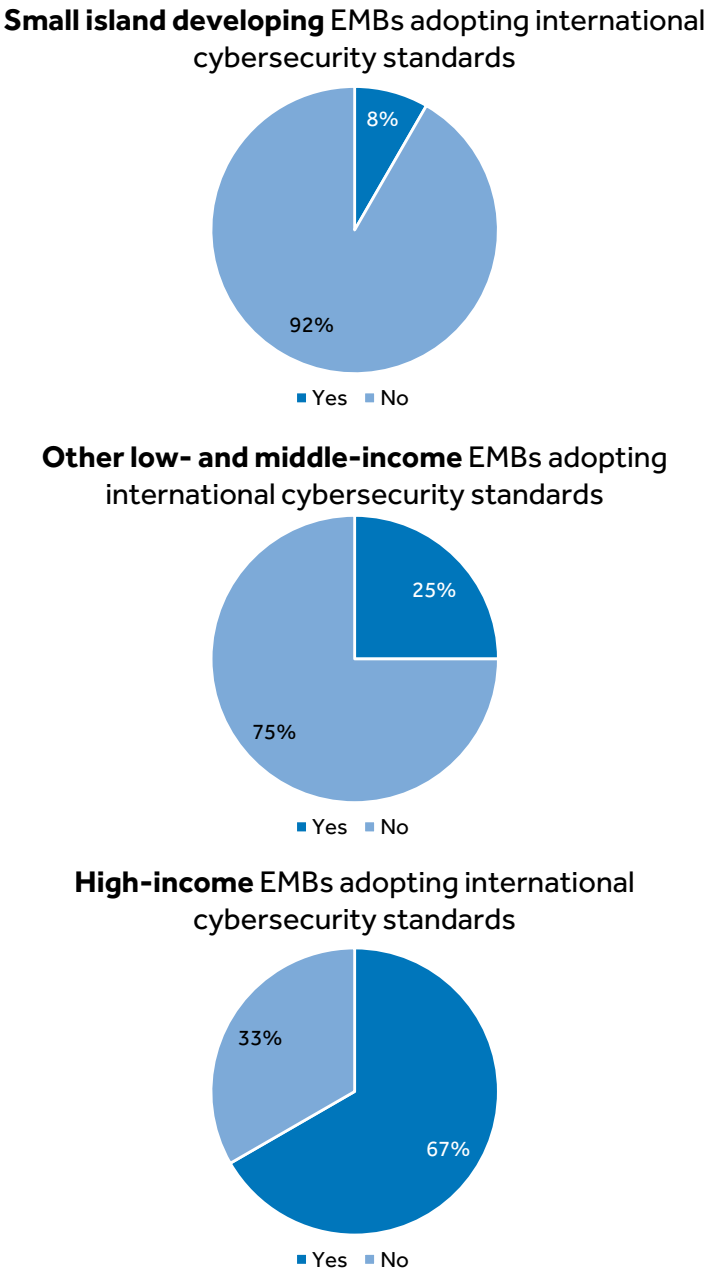
The most widely used series of information security standards is published jointly by the International Organization for Standardization and the International Electrotechnical Commission and is known as the ISO/IEC 27000 series. It provides regularly updated and comprehensive best practice recommendations 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.

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 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.
- **Exercises**: 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

Box 3.11 NIS election exercise objectives

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.'

used more routinely by policy-makers. In either case, EMBs should consider involving key partner agencies and, where appropriate, private sector service providers.

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.

Box 3.12 South Africa's strategic security focus

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.

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 *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.

Box 3.13 Structure and provisions of data protection law

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.

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]

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

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

'levels the playing field between the ruling party and the opposition and can be used to boost electoral transparency and accountability'.[70]

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]

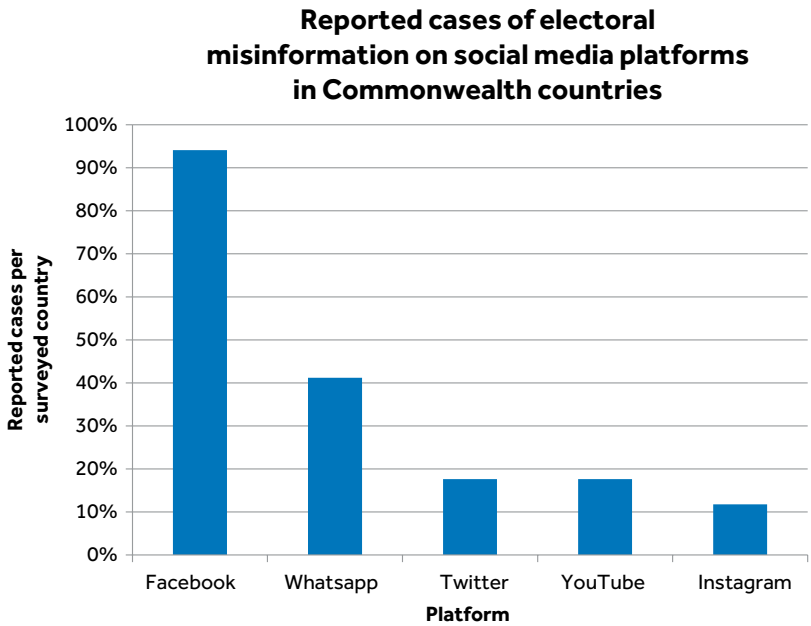
All the respondent Commonwealth countries have experienced the online dissemination of disinformation in relation to their elections processes. Figure 3.7 shows a breakdown of the amount of reported cases per social media platform. We use disinformation to mean 'false, inaccurate, or misleading information 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.

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

Box 3.14 Ghana's approach to voter education

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

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



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.

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

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

Box 3.15 Social media tracking centre during 2016 Ghana elections

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]

these reports within 100 minutes. Platforms are required to take down illegal content notified to them within 15 minutes.

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.

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

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]

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

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

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

(*Continued*)

Box 3.17 Social media codes of conduct and reporting in Commonwealth countries (*Continued*)

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.

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.

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.

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

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

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.

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'

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.

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]

Box 3.19 The EU Code of Practice on Disinformation

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.

Source: European Commission

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.

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]

Box 3.20 Mozilla Foundation recommendations on political advertising archives

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.

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.

Box 3.21 NATO Strategic Communications Centre of Excellence Recommendations

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.

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 #KeepIt On 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.