Chapter 2

Cybersecurity Across the Electoral Cycle

Chapter 2
Cybersecurity Across the Electoral Cycle

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

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

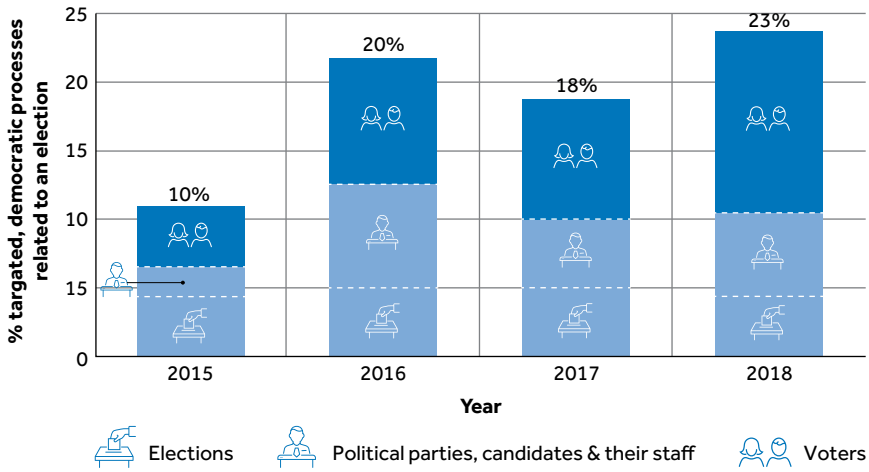
Technology is even more pervasive when considering those participating in the electoral system more broadly. Political parties and campaigning organisations across the Commonwealth now make heavy use of voter data and social media to reach voters via direct marketing and targeted adverts, and of communications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

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

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

- **Threats:** Attacks which undermine the confidentiality of information, the availability of systems or the integrity of processes *(e.g. attacks on voting machines or e-voting).*
- **Vulnerabilities:** Emerging practices which create new attack opportunities *(e.g. the use of electronic voter lists for online targeting by individual candidates using insecure devices).*

Figure 2.1 Cyber threats to global democratic processes, observed by Government of Canada, Communications Security Establishment (CSE)



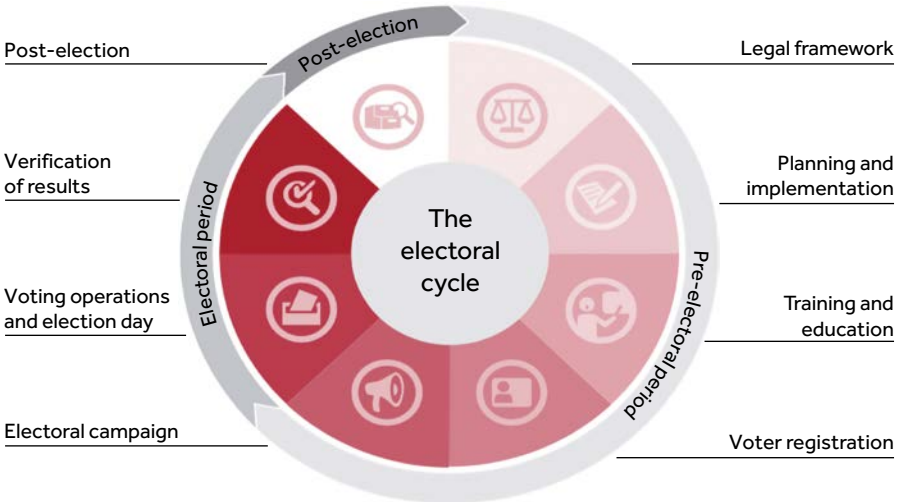
- **Systemic Issues:** Emerging practices which create new incentives for cyberattacks *(e.g. the increased demand for invasive datasets created by online targeting practices)* or a challenging environment *(e.g. a loss of public trust in technology).*

2.1 Election activities across the electoral cycle

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

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

Figure 2.2 The electoral cycle as presented by International IDEA



Source: International IDEA

framework is updated as a response to challenges discovered during electoral processes, as well as encompassing international best practice (as, for instance, from this guide).

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

Box 2.1 Aspects of the electoral cycle vulnerable to cybersecurity risks

	Pre-polling	Polling	Post-polling
Planning and logistics; training and education	Boundary delimitation Polling station placement Recruitment of polling station staff Candidate/party registration/ education Procurement	Disseminating logistical information Disseminating electoral materials	Retrieving results and electoral materials Analysing delays and other issues in specific polling locations Preparing election teams for future

(*Continued*)

Box 2.1 Aspects of the electoral cycle vulnerable to cybersecurity risks (*Continued*)

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

2.2 Overarching features of direct threats

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

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

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

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

Box 2.2 Targeted confidentiality attacks on political parties and campaigns

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

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

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

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

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

For example, while systems are particularly vulnerable to attack when they are connected to the internet, 'air-gapped' systems (which are physically isolated from unsecured networks) are not immune to threats. They may still be accessed physically – by authorised staff or in polling stations, by voters – or compromised by pre-installed software or update processes. Such attack forms are more costly, but are unlikely to deter a determined state actor.

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

Yet both state and non-state actors can engage in electoral interference. It does not require sophistication, technical expertise nor access to resources

to procure cybercrime services in online marketplaces, where malicious actors can obtain the means to carry out distributed denial of service (DDoS) attacks (the malicious flooding of web traffic from multiple sources to overload a system and prevent legitimate requests from being fulfilled) and malware (malicious software, including computer viruses, worms, trojan horses and spyware, among many others).

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

Insider threats

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

Box 2.3 Canadian 2011 robocalling scandal

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

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

One challenge raised by this case is that the plaintiffs had the burden of proving that the cybersecurity-related electoral integrity breach cause a swing in the votes. While the plaintiffs took the unusual step of an automated survey – a robocall to assess the impact of a robocall – to ask citizens about their

(*Continued*)

Box 2.3 Canadian 2011 robocalling scandal (*Continued*)

experiences, the judge was unconvinced.[13] EMBs must be ready to examine complex situations for evidence of the impact of cybersecurity breaches if and when they occur.

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

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

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

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

Recommendation EMBs must model and mitigate the potential of insider attacks, both within their own activities and those of other electorally relevant organisations, such as political parties. Existing anti-corruption efforts, non-disclosure agreements and strong access controls are useful tools in this context.

Recommendation Individuals with reading – and especially writing and administrative – access to significant systems should be security vetted to an appropriate level. While government security agencies may carry out vetting, for independence reasons, EMBs should retain the ultimate decision as to staff appointments.

Maintaining trust

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

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

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

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

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

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

A key requirement in maintaining public trust while introducing new electoral technologies is to ensure that fall-back processes are available if technologies fail during an election. For example, if voter verification devices cannot successfully authenticate one or more voters, how can officials in

polling stations do so, even at a slower pace? If results cannot be transmitted directly by results transmission systems (RTSs), can secure messaging apps on officials' phones be used as a fall-back? And what are the security implications – and potential impact on voter confidence in outcomes – of using such systems? How can the use of these systems be observed and audited?

2.3 Planning and logistics

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

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

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

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

Recommendation EMBs should regularly audit automated systems used for electoral planning for integrity, and put in place processes to ensure documentation and assurance of the provenance of data sources being used.

In the run-up to elections, **systems can also be used to support shorter-term decisions such as the location of polling stations, delivery of ballot papers, and management of staff and volunteers.** There is a greater risk here of successful attacks causing problems to the smooth running of the elections. These systems may be deployed without the knowledge of an EMB, for example, if it utilises the services of a logistics contractor who draws upon

decision-support software, which itself has not been directly procured by the EMB.

Recommendation EMBs should be aware of and seek to mitigate cybersecurity risks involving contractors for electoral logistics, especially those with systems directly linked to the EMB.

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

Recommendation Cybersecurity threat assessment and mitigation should be undertaken regularly by EMBs as part of an ongoing process, rather than in the run-up to ballot periods alone.

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

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

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

Electoral agencies generally have a duty to provide, or support, public information campaigns prior to elections to drive voter registration, and within elections to encourage voters to exercise their democratic rights. In this specific area, disinformation can act to prevent the electoral authorities' message of enfranchisement from being clearly communicated

to voters. Where false information is deliberately used to confuse or prevent potential voters from registering (including for residential immigrants and expatriate voters, where applicable), this can be a serious criminal offence. Disinformation can be used to convince the politically unattached to remain apathetic and not register to vote, or in any case to cast a vote. Suppressing voter turnout can be an effective political strategy and laws in, for instance, the *United States* have targeted voter suppression techniques.

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

Recommendation Information about polling locations should be delivered from EMBs to voters in a secure and robust manner, with monitoring of the veracity and timeliness of information provided.

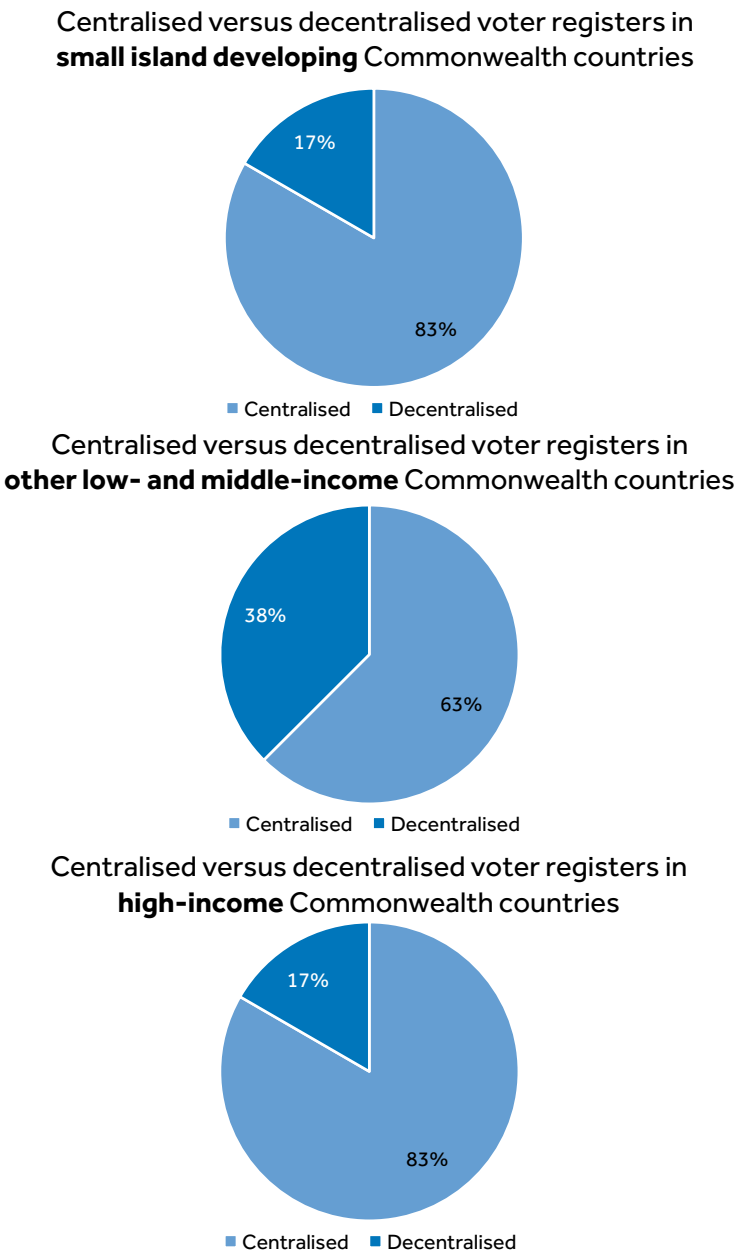
2.4 Electoral rolls

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

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

Furthermore, different members manage electoral rolls at different devolved levels. Some Commonwealth countries give significant authority for roll management to local entities, such as *Bangladesh, Cameroon* and the *UK*, while others, such as *Botswana, India* and *Solomon Islands,* take a more centralised approach. Seventy-seven (77) per cent of the respondent

Figure 2.3 Centralised vs decentralised voter registers in respondent Commonwealth countries



Commonwealth countries adopt a centralised voter register. Figure 2.3 shows the full breakdown across high-income, middle- and low-income and small island developing countries. A national registration database may populate local databases at regular intervals, local databases might be compiled into regional or national databases, or there can be a mixture of both systems.[18]

In many Commonwealth countries, copies of the electoral roll are legally permitted to be provided to *bona fide* campaigns, parties, candidates and representatives. In some members, this roll is open to scrutiny from the public in designated locations, such as local authority offices, and those on the roll may have opted in or out from a commercially available version of the register.

Political parties are potential cybersecurity targets due to their privileged access to voter data. For example, in the *UK*, parties and relevant third parties are eligible for copies of the electoral register for electoral purposes.[19] Similar provisions exist in *Australia*,[20] *Canada*[21] and *Pakistan*,[22] among many other Commonwealth countries. These datasets, containing the names and addresses of the majority of citizens, are of high commercial value and potential sensitivity, and there are often, but not always, significant restrictions related to their downstream use by political parties.[23] Consequently, they are valuable targets.

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

Defending against attacks on the confidentiality of the register is made particularly challenging when the roll is not only in the hands of the EMB and, consequently, it may be at its most vulnerable further downstream. *Mexico*'s Instituto Nacional Electoral (INE) filed criminal charges after an unprotected database of 90 million voter registration records was found hosted on Amazon Web Services. The institute suspected the data had been leaked by one of the political parties, which are given copies.[24] An investigation showed the database had been accessed 2,400 times from 14 internet protocol (IP) addresses.[25] The national Electoral Court fined the *Movimiento Ciudadano* party and two individuals 34 million pesos (£1.4m) for the leak.[26]

To limit the opportunities for misuse of electoral registers, some Commonwealth countries limit the information that is made public. In *Malaysia*, only the last four digits of voters' national identification numbers are included in the published register. In the *UK*, voters can opt out of their records being included in the full public register, appearing instead only in a restricted register used for election purposes and a limited number of

other functions, such as credit referencing. They may also object in writing to political party use of their data.

In *India*, there has been controversy over the publication of a machine-readable form of the register, which already has voter photos and home addresses removed. In *Antigua and Barbuda*, the law has blocked police requests for use of the EMB fingerprint database. Following the 2015 leak in Mexico, the INE limited the information shared with parties to the names of registered voters. The investigation of that leak was aided by the inclusion of 'fingerprinting' data in the copy of the register shared.[27]

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

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

Recommendation An independent agency, such as a data protection authority (DPA), should have competences over the privacy and security of electoral data, including its processing, storage and transformation into derivative data by political parties.

Recommendation EMBs should take steps to ensure that only electoral roll data necessary for the intended purposes of use are transmitted to authorised actors, in a format which does not encourage inappropriate reuse or dissemination and including fingerprinting data to facilitate the tracing of data breaches.

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

Issues around the integrity of electoral rolls predominantly concern:

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

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

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

National digital identities are becoming the basis of electoral rolls in some Commonwealth countries, such as *Pakistan* (see Box 2.5). *Mauritius* has an annual household door-to-door canvas, and the Ministry of IT has designed an 'information highway' to link government agencies, which the EMB can use to check registrations against the civil registry. *South Africa* has a national population registry managed by the Ministry of Home Affairs and each citizen is issued with an identity number at birth. Hospitals report births and deaths, while access to all public services

Box 2.5 Electoral roll integrity in Pakistan

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

requires an ID number. For registration, the ID number is collected through the use of an electronic device and the details and citizen status of the person checked against the national population register. Voter registration is voluntary, but checked against the population registry, and voters can verify their registration online (via website, SMS and/or an app) and check their polling station details. Voters can also view and change their address details online.

While the *UK* does not have a national identity scheme, its Electoral Commission is exploring other mechanisms for automatic voter registration.[28] Elsewhere, in *The Netherlands*, local municipalities maintain a population register which includes each resident's right to vote. This is used to send every eligible voter an invitation to vote before each election, along with details of their polling station.[29]

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

Attempts to avoid fraud in the electoral roll might end up disenfranchising voters. The infamous *United States* 'Crosscheck' system was used to strike off alleged fraudulent voters, until the system was stopped from operating in certain parts of the US on the basis of an injunction from a Federal Court amid concerns about its constitutionality.[30] And a number of African opposition parties have alleged that governments have made it harder for their supporters to obtain national identity documents or otherwise register to vote, by locating registration centres far from areas where they are most popular.[31]

Recommendation EMBs and their cybersecurity partners should identify all avenues, actors and systems which feed into and are informed by the electoral roll(s), and should map out security threats and capacities, contact points and regular procedures to check for data and system integrity.

Recommendation The master copy of the electoral roll(s) should not be connected to public networks and should only be updated with additional information in accordance with procedures designed to ensure the integrity and provenance of the new information.

Recommendation When engaging in data cleaning or validation, the responsible agency should keep complete tamperproof logs of all changes made and use technologies which allow such logging. This allows for detection of integrity issues and specific rollbacks if such issues are discovered.

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

The frequency and means of update to the electoral roll varies significantly across Commonwealth countries, with particular consequences for expectations of availability. Registration methods include automatic, in-person, post, fax and online. The *UK* provides a Register to Vote website,[32] which sends a completed form to the applicant's local Electoral Registration Officer to add to the electoral roll once the application has been validated. *South Africa*'s 1996 Constitution required a national common voters' roll to be created quickly. The Electoral Commission scanned voters' identity document barcodes and used this to retrieve name and voter status from the National Population Register. In only six days, 18.1 million of the 18.4 million applicants were successfully enrolled.

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

Recommendation EMBs and their cybersecurity partners should ensure providers, domain and hosting services for any online registration are easily contactable, identify periods where availability is critical (e.g. near electoral deadlines) and should designate a specific team or individual as responsible to respond to system issues.

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

Box 2.6 Voter registration and availability attacks in the UK

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

2.5 Campaigning

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

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

General targeted advertisements are often run through a process called 'real-time bidding', which consists of an auction for ad placements that is programmatically executed in the milliseconds before a webpage or app loads an advert. This process, in short, sees a browser or application transmit data about the user to an advertising exchange, which passes it on to hundreds or even thousands of agents working for a potential advertiser. The task of these agents is to assess whether the person is 'worth' spending the money to deliver the advert to – for example, if they are likely to click on it or spend time viewing it. To do this, they use a process called '**enrichment**', where the data provided to advertising platforms is passed to a 'data management platform' – whose job it is to combine amassed data of their own, prediction systems and the data of customers (such as political parties) together.[33]

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

Attacks on parties and candidates

The Canadian Communications Security Establishment reported '[c]yber threat actors use cyber tools to target the websites, e-mail, social media accounts, and the networks and devices of political parties, candidates, and their staff'.[34] (*Canada's* intelligence agencies also detected six countries attempting to interfere with political party activity in the 2019 general election via in-person activities.[35]) The *United Kingdom's* National Cyber Security Centre has highlighted three types of attacks aimed at political

Box 2.7 Microtargeting and Cambridge Analytica

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

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

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

- the firm(s) used data obtained through a Facebook plugin created by the University of Cambridge, which scraped data on the friends of those who installed it without their knowledge;
- the firm(s) inferred political opinions of individuals without their explicit consent, which was a violation of the Data Protection Act 1998;
- the firm(s) were unco-operative with the data protection regulators, the Information Commissioner's Office (ICO), refusing to acknowledge its powers or jurisdiction over the data held;
- the activities associated with the firm(s) were funded in a way that was found by the Electoral Commission to breach the law; and
- the firms involved were internationally spread through a complicated corporate structure, such as through affiliated actors in Delaware and Canada, seemingly designed to promote opacity and reduce legal liability.

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

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

parties in the 2019 European elections,[36] which it states are the three 'most common' in recent years:[37]

1. **Hack and leak** attacks aim to steal sensitive information from parties and/or candidates in order to leak it in an attempt to embarrass or discredit those campaigning.

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

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

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

> *'Hacker-for-hire' Andrés 'Sepúlveda's team installed malware in routers in the headquarters of the [Mexican] PRD candidate, which let him tap the phones and computers of anyone using the network, including the candidate. He took similar steps against PAN's Vázquez Mota. When the candidates' teams prepared policy speeches, Sepúlveda had the details as soon as a speechwriter's fingers hit the keyboard. Sepúlveda saw the opponents' upcoming meetings and campaign schedules before their own teams did.*[38]

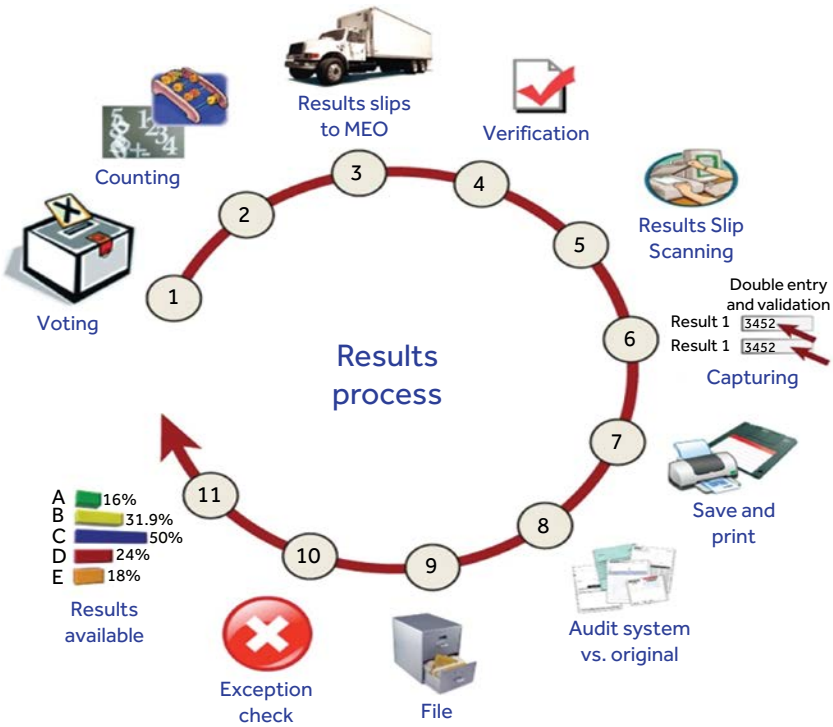
However, more generally, attacks on political parties can undermine the fairness of the election as a whole, with likely spillover effects on voters' perceptions of the electoral machinery and legitimacy of the outcome as a whole. And many parties (and especially candidates in primaries yet to receive party support[39]) have limited technological capability, outsourcing much of their data processing – even in the *United States*.[40]

Recommendation EMBs should ensure the availability of cybersecurity training for political parties, in collaboration with national actors best placed (and seen as legitimate) to deliver such training.

2.6 Voting

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

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



of the result until the voting period ends, to prevent early votes influencing later voters.

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

Voter verification

During polling, election officials check that an individual is eligible to cast a vote at a specific polling station, before issuing them with a ballot paper or allowing them to use a voting machine. In most countries, this is on the basis of a check against a printed register or 'polling book' (or 'pollbook'), against which valid voters are marked off. In some countries, such as *Pakistan*, these registers also include voter photographs based on other state records, such as national identity documents.[41]

Some jurisdictions (such as in 41 of the *United States of America*, and the District of Columbia), use electronic pollbooks, which can be networked to

enable voters to choose a polling place on election day and allow voters to register right up to the election. However, this means the availability of the pollbook system, including any communications links required, is critical to allowing voters to be authenticated. As a backup, EMBs using such systems should ensure a printed list of all eligible voters is sent beforehand to each polling place or that this can be prepared and distributed very quickly. Polling stations in general should have a substantial supply of provisional paper ballots (or equivalent voting machine mechanisms) for those voters that cannot be authenticated in a timely fashion.[42]

Identity document requirements

Not all Commonwealth countries require proof of identity at the polling station. In the *UK (*outside Northern Ireland*)*, identification is not generally required, but ballot papers can later be removed from a count if the eligibility of the voter they are linked to is successfully challenged, since a serial number on ballot paper counterfoils can in such circumstances be used to identify a specific paper.[43] The UK government elected in December 2019 has confirmed plans to introduce a voter ID requirement for elections.[44] *Dominica* is introducing a voter registration card, because the number of registered voters is greater than the population.

In other countries, such as *India, Trinidad and Tobago,* and *South Africa*, a mechanism to prevent duplicate voting is for voters to mark a specific finger or fingernail with an indelible ink that will take several days to disappear, aa shown in Figure 2.5.[45]

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

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

There have been concerns in some countries that minority groups which already under-participate in polls are less likely to possess proof of identity and will therefore be further disadvantaged. In *UK* trials in May 2019, between 0.03 and 0.7 per cent of voters turned away for lack of ID did not return to vote. In two areas, there was a correlation between the proportion of each ward's population with an Asian background and the number of turned-away voters.[46]

Given extremely low levels of impersonation fraud in previous *UK* elections, there were criticisms of the government's plan to mandate the requirement across the country from equality advocates and from the opposition, with one Member of Parliament (MP) claiming the requirements were an attempt 'to suppress voting, and … designed deliberately to hit the poorest hardest'.[47]

In the *United States*, a recent large-scale study concluded voter ID laws 'have no negative effect on registration or turnout, overall, or for any group defined by race, gender, age, or party affiliation', but 'have no effect on fraud either – actual or perceived'.[48] One follow-up study suggested there was some evidence that increased voter mobilisation efforts by the Democratic Party in affected areas counteracted a negative turnout impact of voter ID requirements, although this was rejected as an explanation by the first study.[49]

Biometric authentication

Globally, multiple voting by individuals remains a serious problem for elections.[50] A number of Commonwealth countries, notably *Cameroon, Ghana, Jamaica, Samoa* and *Pakistan*, have used biometric authentication devices to verify the fingerprints or other physiological characteristic of voters at polling stations, registered prior to the election, and to prevent duplicate voter registrations. If connected, these machines can also prevent duplicate voting during polling by individuals – but this brings its own reliability and security risks.

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

Box 2.8 Biometric voter verification trials in Pakistan

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

In the Pakistani context, there is a lack of evidence in the existence of the specific problem that biometric authentication is designed to solve. In the general elections 2018, where no biometric systems were used, there were no complaints to the Election Commission concerning voter identification issues. Indeed, there used to be a challenge because political pressure meant that it was optional for women to have photographs on voter lists, which would cause problems for the Election Commission's preferred mode of verification and would have proved an area of controversy concerning allegations of fake votes. This, however, was remedied, and now photographs are obligatory for all on the voter lists. Yet there was considerable wariness of using biometric verification machines with no clear problem identified, particularly following controversies in Kenya and Nigeria concerning these machines.

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

levels of 'false positives' (where an individual is wrongly accepted) and 'false negatives' (where an individual is wrongly rejected).

A review by Cheeseman et al. concluded 'as a rough rule, biometric registration has tended to work better than biometric verification, simply because the time pressure is so much more intense when millions of voters have to be processed in a single day'. This was apparent in *Chad* in 2016, where the new register apparently eliminated much double registration, but actual voting was still chaotic. In *Kenya's* 2013 elections, a new biometric registration process worked relatively well, producing a register that appeared to have been more transparent than any previous one – although voter identification machinery failed at some point in more than 50 per cent of polling stations.[51] But despite biometric registration, multiple registration still happened in *Somaliland* in 2008 (since the EMB 'did not use the automatic fingerprint recognition software for reasons related to its cost and organizational problems'[52]) and in 700,000 cases in the *Democratic Republic of Congo* in 2011.[53]

Specific biometric technologies can also work less well for some groups – for example, fingerprint recognition often has difficulty with elderly people and manual workers' reduced fingerprints.[54]

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

> *In polling stations with a randomly assigned election observer, [biometric identification] machines were about 50 per cent less likely to experience breakdown as they were in polling stations without observers. We also find that electoral competition in the parliamentary race is strongly associated with machine breakdown. Machine malfunction in turn facilitated election fraud, including overvoting and ballot stuffing, especially where election observers were not present.*[55]

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

Recommendation Given the potential cybersecurity implications of requiring biometric or other electronic identification systems, EMBs should gather a clear evidence base on the impact on fraud, turnout and system impact, particularly among marginalised communities.

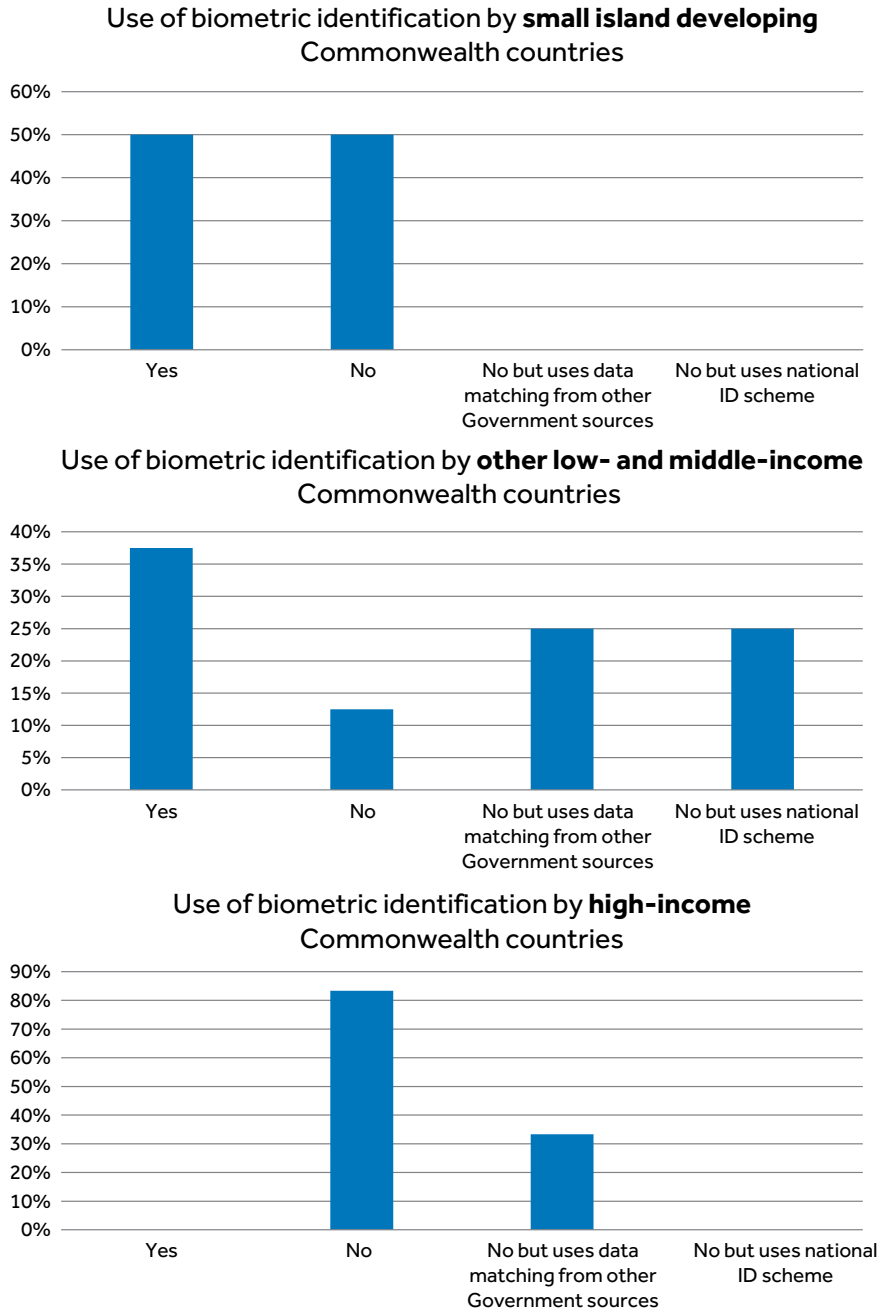
Vote casting

Most Commonwealth countries – 88 per cent of respondents – require voters to hand mark ballot papers in a physically concealed location in a polling station near their home, or at an embassy or consulate, before placing completed papers in a locked ballot box. Figure 2.8 shows the types of voting seen across country groupings in respondents. Using pencil/pen and paper obviously minimises cybersecurity risks.

Secret ballots reduce the pressure being put on voters to cast their vote for a specific candidate, since they cannot prove afterwards to third parties how they have done so. While over a century old, this mechanism remains critical to fair elections and good governance, since 'multiparty politics in counterfeit democracies often resembles a competitive plutocracy, in which power is wielded by the wealthy' – the rich buy electoral races and governments divert funds to buy votes – 'and poorer citizens rarely secure high political office'.[56]

To protect ballot secrecy, voters are required not to take photographs of their ballot paper – although this has become more of a challenge for election

Figure 2.6 Use of biometric identification by respondent EMBs



officials given the modern prevalence of smartphone cameras. (Many countries allow some or all voters to cast votes by post or a nominated proxy, particularly those who will be away from polling stations at election time.)

Some Commonwealth countries, notably *India* and *Bangladesh*, use machines in polling stations to record votes from some or all voters. A breakdown of

Box 2.9 Stolen biometric voter registration kit in Malawi

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

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

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

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

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

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

India's electronic voting machines (EMVs) were developed during the 1990s by a state-owned corporation, and introduced into elections from 1998 in an attempt to reduce the incidence of widespread ballot-stuffing (whereby polling stations were taken over by political activists, who inserted false ballot papers into ballot boxes before they were counted). EVMs limited the rate at which votes could be cast to five per minute and featured a 'close' button to disable the device if violence was threatened. The machines also took an impression of voters' thumbprints, which were stored afterwards in an accessible register. Collectively, one study found these measures led to markedly lower numbers of (real plus fake) votes being cast and reduced the vote share of incumbents, as well as eliminating votes rejected because they were incorrectly marked. Turnout of vulnerable voters increased.[57]

Following concerns about EVM reliability and fraud, in 2011 the Indian Supreme Court ordered the Electoral Commission to consider whether EVMs should produce a voter verifiable paper audit trail (VVPAT) that could be used to check machine counts, ordering in 2013 that these should be introduced.[58] VVPATs were developed and trialled in the 2014 general election, with their use gradually extended to all assembly and general elections. For the 2019 general election,

(*Continued*)

Box 2.10 The interaction of electronic voting machines and fraud in India (*Continued*)

the court ordered that the VVPAT results should be checked against the totals recorded by the EVM for five randomly selected machines per assembly segment, a five-fold increase over the previous Electoral Commission plan of checking 4,125 machine results. The commission estimated this would delay the announcement of results by around four hours.[59]

the different types of voting employed across respondent Commonwealth countries is included in Figure 2.1. *India*'s experience with electronic voting machines is described in Box 2.10.

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

The *United States* is an example of a country with an extreme diversity of vote casting and counting machines, which are managed by individual counties, as shown in Figure.[60] Recent analysis by *Politico* has shown that of the 596 states (with centralised processes) and counties (with county-run processes) using paperless voting machines tracked, 84 planned to replace them; 82 were in the process of doing so; 35 had completed the switch; 193 had no plans to do so; and 202 did not respond to inquiries.[61]

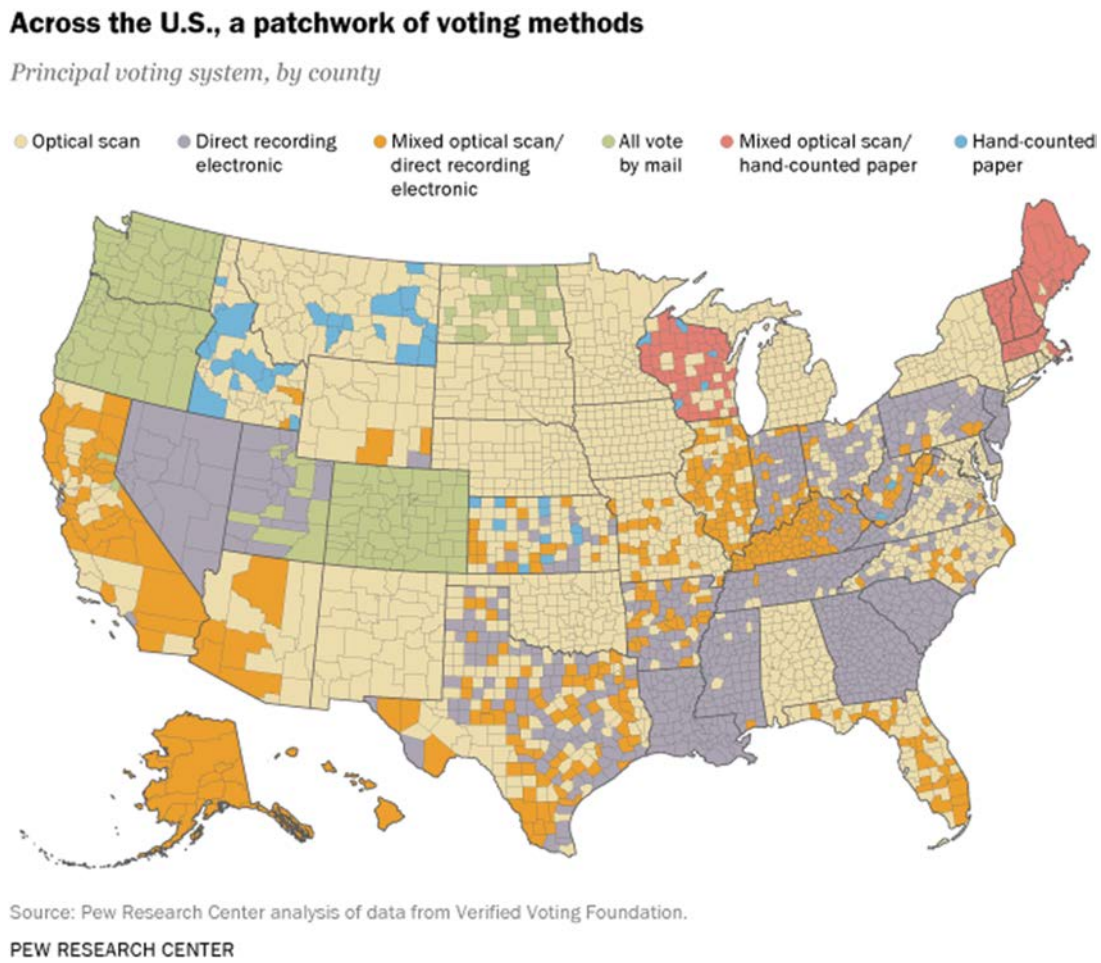
DRE systems can instantly tally all votes cast when polls are closed and transmit them electronically to central counting points via mobile data, internet connectivity or other means (such as satellite links in rural areas with limited connectivity). They also eliminate the cost of printing and distributing ballot papers and can provide accessibility support to visually impaired and other voters. However, they can suffer from all of the cybersecurity risks familiar to internet users, even when carefully configured and operated. It also therefore makes them vulnerable to accusations of hacking, even if they are actually secure, potentially impacting voter trust. They are expensive to initially purchase and require ongoing technical support and upgrading.[62]

Polling stations using DREs should have a substantial quantity of paper emergency ballots available, so voting can continue while any faults are remedied.[63]

Voter verified paper audit trails

Because of these potential problems, a number of non-Commonwealth countries have cancelled pilots or moved away from the use of DREs in the last decade, including *Ireland*, the *Netherlands* and *Germany*.[64] The US

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



National Academies of Sciences now recommends: 'All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election'.[65] Retaining **paper ballots** or providing a **voter verified paper audit trail** for voting machines (as required by *India's* Supreme Court in 2013, described in Box 2.10) provides a critical backstop for forensic investigation, court judgments and ultimate public trust in election outcomes.

Even where VVPATS are produced by a machine following an electronically cast vote, the limited research that has taken place so far shows that voters take little notice of them.[66,67] The US National Academies of Sciences concluded that asking voters to hand-mark ballot papers would more likely lead to their vote being recorded accurately.[68]

Germany's Constitutional Court determined in 2009:

> *The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject […] The very wide-reaching effect of possible errors of the voting machines or of deliberate electoral fraud make special precautions necessary in order to safeguard the principle of the public nature of elections.*[69]

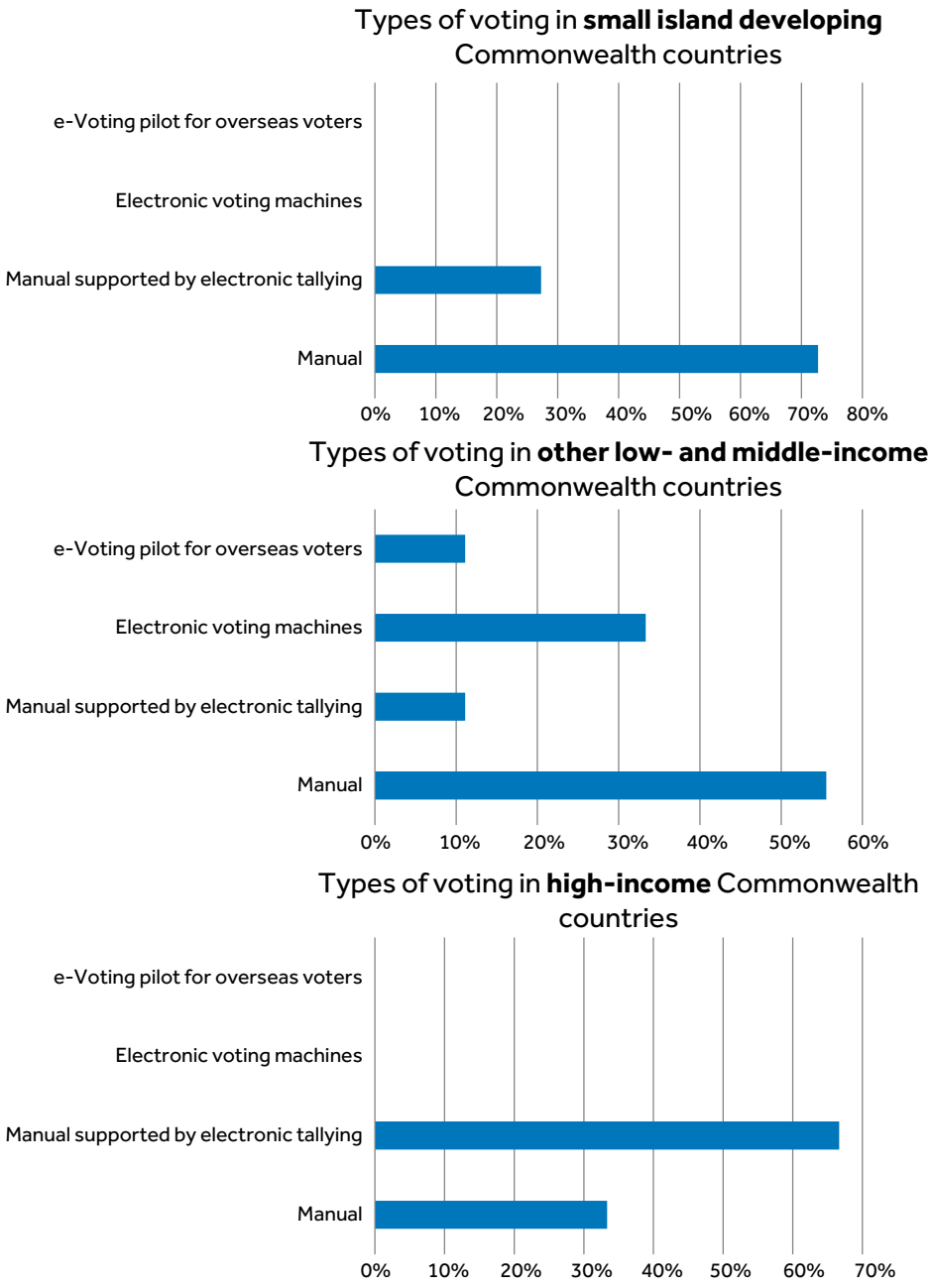
Following claims of election hacking in one African Commonwealth country in 2017:

> *the limited knowledge of many citizens and commentators regarding how digital processes actually work meant that it was extremely difficult to differentiate false claims from plausible ones. This was revealed in comical fashion when the opposition claimed to have a print-out of the log of activity on the [EMB] servers and distributed it at a press conference only for none of the media, analysts and observers present to have the skills necessary to be able to tell if it was genuine.*[70]

Recommendation Where machines are used to cast votes, EMBs should carefully consider the use of voter verified paper audit trails to enable every vote to be verified where results are disputed.

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

Figure 2.8 Types of voting employed across respondent Commonwealth countries



Yet regular surveys by the *UK* Royal National Institute of the Blind (RNIB) have found many of the UK's 350,000 blind and partially sighted voters to be unhappy with the assistive devices provided, with only one in four respondents feeling they were able to vote independently and in secret in the 2017 general election. Only 1 per cent of visually impaired people use Braille.[71] The RNIB is campaigning for the government to 'Provide an online and/or telephone option for blind and partially sighted people to cast their vote independently and in secret if they aren't able to vote at their polling station' in time for the next general election.[72]

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

Remote voting

Remote voting has been used in a number of different countries, for reasons ranging from convenience to reaching voters who are conventionally disenfranchised in practice, such as overseas voters. Non-residents can vote in almost half of the respondent Commonwealth countries, though the figure is much lower for small island developing states (see Figure 2.9). Methods for overseas voting that have been deployed by the 115 countries worldwide that, as of 2007, had some remote voting provisions include:[73]

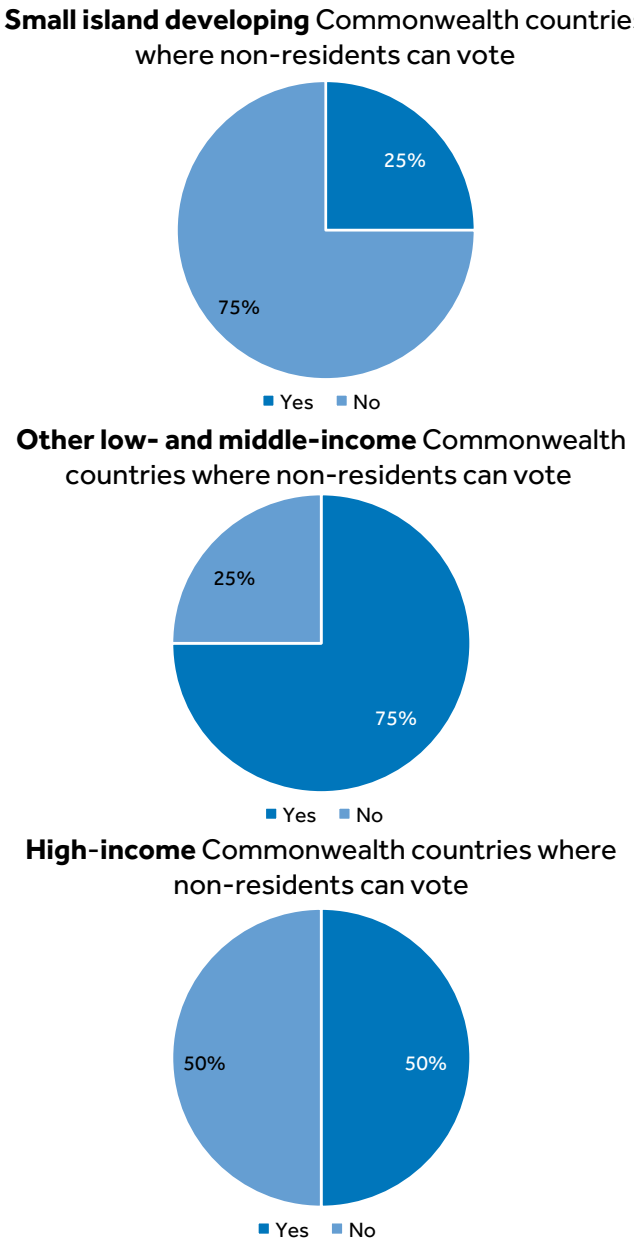
- personal voting, for example, at representations, consulates and embassies;
- postal voting;
- proxy voting;
- voting by fax; and
- internet voting (e-voting or i-voting).

Box 2.11 India's electronically transmitted postal ballot system

India used a hybrid model for remote voting, which it refers to as an 'electronically transmitted postal ballot system' (ETPBS). This service was first provided to armed forces/services voters and overseas electors, who can register online and also receive ballot papers electronically – which are then printed, completed and physically posted to returning officers. The ballot includes an encrypted QR (Quick-Response) code which can be scanned when the vote is counted.[74]

Recommendation Where non-resident citizens are enfranchised, provision of online electoral information and forms for printing and returning by post present significantly lower cybersecurity risks than remote voting.

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



Internet voting

Estonia famously allows votes to be cast from individuals' own computers. Very few other countries have taken this step (*Switzerland* has allowed it for cantonal votes, although Swiss Post recently suspended its system following the identification of security problems by computer scientists,[75] and the *Netherlands* has trialled this method in the past[76]). Estonia is unique in the

level of electronic ID, smartcard readers and other infrastructure it already has in place, for the use of a whole range of government services.

Estonian voters can check how their vote has been recorded using their smartphone – reducing although not eliminating the chance it has (accidentally or deliberately) been recorded incorrectly. Voters can also cast multiple votes, with only the final vote being recorded, to reduce the opportunity for voters being pressured into voting in a specific way; 17.6 per cent of eligible voters cast their votes this way in the May 2019 European Parliament elections.[77]

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

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

> *At the present time, the internet (or any network connected to the internet) should not be used for the return of marked ballots. Further, internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the internet.*[78]

Recommendation Before introducing internet voting systems in elections, EMBs should assess very carefully the cybersecurity risks they introduce, as well as the extensive mechanisms required to manage that risk and potential damage to voter trust in case of disputed outcomes.

Vote counting

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

Where results are extremely close, candidates may commonly request recounts. This is important for accuracy, given that hand counting is an

Box 2.12 Internet voting trials in Pakistan

The topic of the practical arrangement of voting rights for Pakistani citizens has a long history of political discussion. Constitutionally, Pakistani citizens living overseas retain a right to vote, as residency is not a constitutional requirement.[79] In 1993, a petition was filed in the Pakistani Supreme Court where a British-Pakistani law student, Yasmin Khan, sought the right to vote overseas.[80] This petition was heard, and passed to the ministries and the Election Commission to discuss, but ultimately nothing came of it in the subsequent years. Two similar petitions were filed in 2011, calling upon the Supreme Court to issue directions to the Election Commission to prepare electoral rolls for overseas Pakistanis and to take 'appropriate measures for making it possible for the Overseas Pakistanis to cast their vote in Pakistan consulates and embassies'.[81] This led to a request to the Election Commission to undertake such consulate/embassy voting for the 2013 general elections; however, it was not given enough lead time to securely carry this out. The run-up to the 2018 general elections saw the passing of the Elections Act 2017, which addressed the issue in part, permitting the Election Commission to 'conduct pilot projects for voting by Overseas Pakistanis in bye-elections to ascertain the technical efficacy, secrecy, security and financial feasibility of such voting',[82] without specifying the type of voting to be used.

Pakistan had already trialled voting from embassies and consulates and was aware that while this might work for Pakistani expatriates in the United Kingdom where population density allowed strategic organisation of polling stations abroad, it would be much more challenging in places where diplomatic infrastructure was sparser or populations were more distributed. There were also plans concerning voting by voice – 'tele voting with interactive voice response' – and 'postal ballot using email', which were led by a parliamentary committee in 2015, but these were ultimately not pursued further, in particular following a joint report from the Election Commission and the Ministry of Foreign Affairs about their security and integrity flaws.[83]

Pakistan then considered internet voting or 'i-voting', and there was some pressure to enable overseas voting, in particular i-voting, for the general elections of 2018. However, the Elections Act 2017 only stated that pilot projects 'may' be run and in any case in 'bye-elections'.[84] The Supreme Court determined that the constitutional right of Pakistanis overseas to vote should make these obligatory pilot schemes rather than optional for the Election Commission, and that it should undertake these through its rule-making powers.[85] The pilot schemes need not be restricted to internet voting; there was a mandate for many different approaches to be trialled by the Election Commission. The Election Commission in August 2018 appealed to the Supreme Court to ask that these voting tests be 'pilots' in the sense they had been for the use of biometric verification and voting machines (see below) – that the votes should not count towards any final tally. This was refused by the court.

As a result of this refusal, a series of by-elections that were run in October 2018 *were* undertaken with overseas Pakistanis able to vote through a new 'iVOTE' system. The Electoral Rules were changed in September 2018 to include details of this system, which states that the current policy for voting by overseas Pakistanis is internet voting.[86] Overseas Pakistani voters holding a NICOP identification card, machine readable passport and with an email address, can register with these details, face security questions and be provided with a passcode for voting before polling day. Voting is only open on polling day, as per

(*Continued*)

Box 2.12 Internet voting trials in Pakistan (*Continued*)

Pakistani law.[87] The results of these ballots are to be held separately from other votes until the Election Commission is satisfied that the 'technical efficacy, secrecy and security of the voting' has been maintained. At this point, they could be included in the consolidated results.

Internet voting would not be without hazards in Pakistan. Calculated evenly and simplistically, the approximately 6.7 million overseas voters represent just under 20,000 individuals per constituency. In the general elections of 2018, the authors of this report calculate that 32.6 per cent of National Assembly constituencies had a margin of victory of under 10,000; 43 per cent had a margin of under 15,000; and 51.9 per cent had a margin of under 20,000.[88] Individuals are able to vote when abroad in their 'permanent residency' in Pakistan, which is an address (e.g. place of birth) which cannot be changed, unlike their 'temporary address' which may be their place of residence in the country. As a result, it is clear that overseas citizens in Pakistan have considerable political clout. Equally, a controversy of security or integrity of the overseas ballot, when spread across the whole country, comes with the potential to create doubt or distrust in the results of the entire election.

The software used in the i-voting scheme, iVOTE, was an in-house development of the National Database and Registration Authority (NADRA), the agency under the Pakistani Ministry of Interior that regulates government databases, issues and manages the identification system used in Pakistan, and which worked with the Election Commission on the computerised electoral rolls. NADRA has considerable experience and infrastructure for software development and has developed software systems and processes for other Commonwealth countries, such as the Kenyan electronic passport system, the Bangladeshi driver's license system and the Fijian electoral management system, among others.[89]

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

NADRA's proposed solution to this was to use the numbers on machine-readable passports as a verification method in co-ordination with a NICOP number. This was known as the remote identity proofing (RIDP) system.[90] The iVOTE system subsequently developed (in Java) was tested for three months in-house by NADRA's lead penetration tester as a first approach to analysing its security. The iVOTE system was demonstrated to the Supreme Court on 12 April 2018, in a session including a variety of political parties, computing academics from Pakistani universities, citizens and media outlets.[91]

This was followed by an external task force, the Internet Voting Task Force (IVTF), which was established by an order of the Election Commission, 'mandated to

(*Continued*)

Box 2.12 Internet voting trials in Pakistan (*Continued*)

assess the overall web-based automated system of internet voting for eligible Pakistani voters living abroad'.[92] This task force was to audit and evaluate the system for various vulnerabilities. The task force included primarily academics and a Dubai-based firm, IT-Butler, run by a Pakistani national that the Election Commission also used for training and the seeking of international cybersecurity standards and certification. The IVTF Report that resulted from this study, which is publicly available, highlighted a range of concerns, including the following:

- iVOTE did not provide the ballot secrecy required in the Constitution of Pakistan and in the Elections Act 2017.[93] This was inherent to the computational approach taken in iVOTE, rather than a failing of the software implementation.
- Voter coercion and vote buying were very possible in this system.
- A particular vulnerability was allowing users to choose their constituency within the voting system outside of that which they are registered.
- The website and interface were vulnerable to being impersonated in phishing attacks.
- The DDoS-protection utilised by NADRA could compromise ballot secrecy, exacerbated by the foreign nature of the external provider.
- iVOTE employed deprecated and compromised third-party components.
- No usability studies had been carried out, particularly in relation to low-literacy individuals, which in turn might raise new security concerns.
- iVOTE emails could be blocked by spam filters.
- iVOTE did not offer the verification or redundancy features in other jurisdictions with experience in internet voting.
- There was no threat model analysis or code documentation.
- There was no known resource planning for monitoring iVOTE on polling day.
- There was no known planning for preventing insider attacks.
- Newer technologies and architectures should be considered.

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

Following this report, which was then presented to the Supreme Court and to the ECP in May 2018, the Supreme Court ruled that such a system should go ahead and be trialled in the impending by-elections in October 2018. These by-elections represented 35 constituencies, which were electing 11 National Assembly seats and 26 Provincial Assembly seats. Some 639,909 overseas

(*Continued*)

Box 2.12 Internet voting trials in Pakistan (*Continued*)

Pakistanis would have been eligible to vote for these by-elections, of which in the relatively short 17 days available for registration, 7,419 registered (351 of which were later excluded due to their constituencies running unopposed). Video tutorials on how to use the system were provided in English and Urdu.[94] Of those remaining, 6,223 exercised their voting rights on polling day itself: an 83.54 per cent turnout rate. The Election Commission was aware few registered, but the cause of this was unclear. In particular, it was unclear whether there was little demand from outside the country (compared to the considerable political appetite for overseas voting from some actors within the country); whether by-elections were not interesting or salient enough democratic events; or whether there was limited awareness of the iVOTE system. In the end, following reflection on the process, the Election Commission did not exercise its powers to ignore these votes for reasons of technical efficacy, secrecy or security, and instead included the votes into the final counts.

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

The report of the scheme[95] was laid before parliament on 14 January 2019. At the time of writing, Pakistan was waiting to see if parliament would agree to internet voting in future elections, particularly given the implications for ballot secrecy, which is particularly sensitive given the risk posed by those in coercive positions, such as heads of households or ringleaders or co-ordinators of labourers, gathering votes and using them collectively. Whether the iVOTE scheme is expanded to a general election was at the time of writing in the hands of parliamentarians and would require an amendment of the Elections Act 2017 to expressly permit.

extremely repetitive process where small mistakes can easily be made, even while maximising the transparency of the process.

In some Commonwealth countries, such as *Australia* and *Malta*, optical scanners are used to rapidly count votes marked on ballot papers.[96] This can particularly increase the speed of counting where proportional voting systems are used, and voters can specify preferences between a number of candidates.

In *Kyrgyzstan*, voters place hand-marked ballots into a scanner which reads the vote, then deposits accepted papers into the main 'bin', diverting rejected ballots into a special 'bin'. When voting closes, the scanners are connected to the internet, displaying the results and sending them to the Central Election Commission (CEC). A hand count is performed and the ballots in the rejected bin are added to the main count if their intention is clear. The results of the hand count are sent to the CEC when complete and, in case of discrepancy, the hand count takes precedence.[97]

In the *UK*, many returning officers use digital systems to help verify the voter information and signature on the outside of an inner envelope containing postal ballots, before valid ballots are delivered to the relevant counting centre to be included after the close of polling. Lack of public understanding of this system – despite extremely clear public information from the Electoral Commission – led to thousands of tweets following the December 2019 general election questioning why a company with a board member linked to one party had been counting postal ballots (it had not).[98] There were also public (unproven) claims about voting patterns on postal ballots before polling day, repeated to great controversy by the BBC's political editor one week before the election.[99]

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

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

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

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

Risk-limiting audits

The concept of 'risk-limiting audits' has emerged as a best practice in EMB approaches to efficient results auditing, where machines are used to cast and/or count ballots.[100] Before the result is certified, a fraction of such ballot papers are selected for hand counting, to compare against the machine totals. The sample size (percentage of randomly selected ballot papers) is increased as the margin of victory for the winning candidate or party decreases, ensuring the optically scanned and hand-counted results match to within an agreed statistical margin of error. Basic additional checks can also be carried out, such as ensuring the number of votes cast corresponds to the same number of votes marked off in poll books.

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

2.7 Communication of results

Digital communication of results by election officials once they are counted – preliminary and final – presents significant opportunities for attacks on electoral integrity, but also opportunities to make information (such as photos of preliminary results sheets) more widely available and hence effective as a tool for third parties to detect fraud. 'Parallel vote tabulations' are often undertaken by political parties, the media and electoral observers, and are an important tool for improving the reliability of results reporting.[101]

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

Transmission

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

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

Box 2.13 Vote counting and collation in Ghana

In **Ghana** vote counting and collation is done manually. Results are collated by district, constituency and then finally nationally at the Electoral Commission of Ghana's (ECG) headquarters. Returning officers use fax initially. The ECG waits until the manual process of checking, collating and delivery is completed before announcing the certified results. This process can often take up to 72 hours, to allow delivery from remote areas that are not easily accessible. As polling stations and collation centres are required to display results once they have tallied votes, parallel systems for the collation and transmission of votes have been set up by both parties and the media. While some interviewees noted that this transparency measure proves vital for preserving trust in the elections process, it often means there is a large gap in the reporting of the provisional and certified results – and this leads to public frustration and periods of political instability. Consequently, the ECG is trialling new forms of transmission in order to speed the process up.[102]

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

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

As with all the other aspects of the electoral cycle, connection to networks that involve the transfer of data from one component to another will

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

Without enough time for testing, one African Commonwealth country found in a 2013 election '[e]arly result transmissions recorded a remarkably high number of rejected ballots; it was then announced that the system had arbitrarily multiplied the number of rejected ballots by eight, though how and why has never been explained. Then, following an initial stream of results, the flow of information ground to a halt'.[103] And in *Azerbaijan's* 2013 election, 'the credibility of a mobile phone app purportedly designed to communicate results was fatally undermined when it released the figures a day before a single ballot had been cast'.[104]

Recommendation EMBs should ensure results transmission systems (RTSs) are secure, subject to clear and strict access controls, and have appropriate levels of redundancy and backup procedures in place should components of them unexpectedly fail. Final results certification should depend on verification of original signed count forms.

Recommendation EMBs can improve the resilience of results reporting, as well as public confidence in the results, by supporting parallel vote reporting and tabulations by civil society organisations.

Tabulation and aggregation

Tabulation systems will be required to aggregate votes in cases where vote counts are centrally located. This will often involve the use of dedicated software to tally transmitted vote data. Such software must be properly audited and tested before use. Any changes should be carefully documented and subject to version control, and sufficient training must be provided to users of the chosen tools.

Approaches using common and easily changed software, such as spreadsheets containing automatic formulae, are prone to alteration. Public sector best practice in maintaining software such as this should be followed. Following a scandal involving incorrect spreadsheet formulae in a procurement process,

the *UK* created processes for providing quality assurance to high-risk spreadsheet-based tools in its 'Aqua Book', many elements of which will apply even to simple and predictable tabulation approaches.[105]

Box 2.14 Results transmission in Pakistan

As a large country with a constitutional requirement to hold elections in a single day, as well as a history of disrupted democracy, in **Pakistan** the system for transmitting results in a reliable form emerged as an important political concern. The Elections Act 2017 in Pakistan introduced a new, photographic mechanism for results transmission. Presiding officers have been trained to use a smartphone app to photograph 'Form 45' – the document which was manually taken from polling stations to a central centre under the pre-existing system. In the 2018 Pakistani general elections, 51 per cent of results were sent through the new system. In some areas, the installation of satellite internet was required. On polling day, an attempted denial of service attack on the transmission system was thwarted.[106]

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

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

Publication

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

Further information can also be provided to increase election transparency – for example, *Malawi*'s EMB publishes images of all results sheets on its website, enabling third parties to check for any signs of fraud and promoting public confidence in results.[107]

Attackers can conduct denial of service attacks on a results portal, just as they can for any public facing website, making reporting unavailable and thereby

undermining voter confidence. The data is also subject to manipulation if attackers gain unauthorised access. Another possibility is that voters are redirected to spoof websites which purport to demonstrate official results.

> *In one African Commonwealth country 2017 election, 'results quickly began to flow into the online system, which was connected to a new – and impressive – website that allowed citizens to search results to the polling station level. However, as more information about the election began to trickle out, it transpired that some parts of the system had not been strengthened. Most notably, around a quarter of the scanned forms were not transmitted and made available by the time that the election result was announced. It also transpired that the passwords of senior election officials were used to access the system thousands of times – potentially by different people'.*[108]

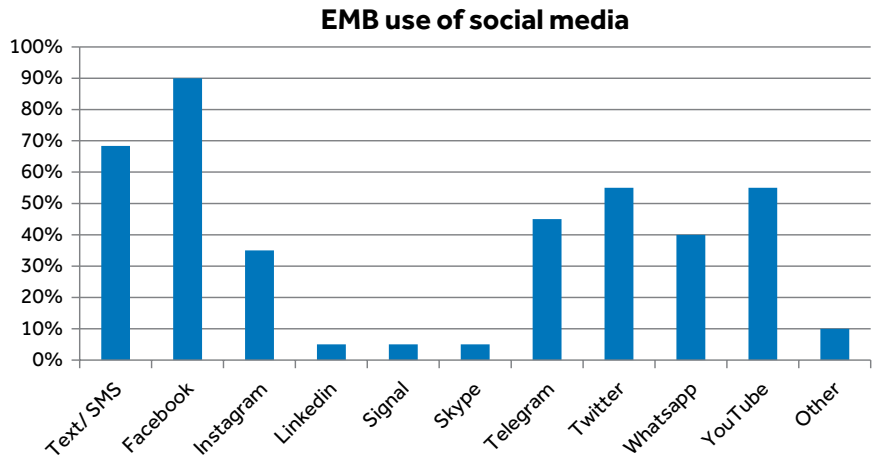
Although in all Commonwealth countries there are multiple sources of media reporting and therefore no one single point of failure, broadcasters and online news outlets still pose a vulnerability – particularly if a sophisticated actor had the means to conduct simultaneous attacks on multiple outlets. Even if the correct results can be broadcast effectively in time, there is a risk of immediate disruption or violence. In one example of a narrowly avoided incident, Russian-speaking hackers compromised the website of *Ukraine*'s Central Election Commission, changing the result, which was noticed and corrected by officials just one hour before it was due to be announced. Despite this, the fake result was broadcast by Russian state media.[109]

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

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

It is of course open to electoral authorities acting unlawfully to simply announce results that do not correspond to the votes cast. In the August

Figure 2.10 Respondent EMB use of social media



Box 2.15 Results reporting in India

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

The commission also displayed the real-time results of the election on its mobile app, allowing users to see the authentic results directly from their phone, anywhere. The user could view these results by scanning the barcode of their commission-issued voter-ID. The Election Commission had designed this innovative mobile application, which was called the Voter Helpline. This mobile application connected five databases together and prepared seamless services for citizens; it allowed searching of their names from the 910 million in a fraction of a second. The voter could verify their name, the polling station, details on the voter card and also the election schedule. If they already had a voter ID card, simply by calling the voter ID card the details can be verified.

2017 vote in *Venezuela* for a new constituent assembly, the Electoral Council announced that 8.1 million people – 41.5 per cent of the electorate – had voted in favour of the new assembly. But the CEO of the company Smartmatic, which provided the voting machines used, reported this figure had been inflated by at least one million voters.[110] *Reuters* reported an internal memo from the council stating only 3.7 million votes had been cast two hours before polls closed. The country's chief prosecutor stated: 'I'm absolutely sure that those numbers are not correct'.[111] In a second example

from the 2018 presidential elections in *Democratic Republic of Congo*, analysis by the *Financial Times* of tallies from 62,716 voting machines obtained from the Electoral Commission's central database, as well as a parallel vote tabulation conducted by 40,000 observers from the Catholic Church, demonstrated the second-placed candidate had been wrongly announced as the winner.[112]

Both cases demonstrate that careful analysis of the large volumes of data produced by voter authentication and casting systems can be used to detect electoral fraud. A Congolese Electoral Commission whistle-blower, 'imprisoned and tortured for nine days in the DRC' in 2017, has since been given refugee status in the UK.[113]

2.8 Auditing and challenging results

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

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

Archiving of systems, processes and outcomes is crucial, but electronic archives in particular might also be subject to attack, particularly with an aim to destroy or tamper with them. While EMBs commonly have data retention systems in place for the safekeeping of physical or paper resources used throughout the electoral cycle,[114] systems for storing and safeguarding electronic data are likely newer and may not be as complete as desirable for such audits. Important data to audit might include:

- 'snapshots' of the versions of any critical software or firmware deployed during the election on, for example, voting machines, biometric verification machines or tabulation systems;

- copies of relevant e-polling books, in accordance with laws on retention governing electoral rolls;
- appropriately granular voting data, well organised alongside metadata and clearly documented;
- instructive documentation, including online documentation and guidance, provided to staff and volunteers; and
- web logs from critical systems.

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

> *Rather than aiding transparency, the extremely high level of IT knowledge and expertise required to understand how integrated electoral management systems work, and what is implied about the process if they do not, means that opposition parties and international monitors are often poorly placed to evaluate the quality of the process – even in relatively technologically savvy states.*[115]

A common misperception is that the release of information about system security can reduce that security and that transparency can create new vulnerabilities. One can assume that any adversary should know these details already and that transparency can instead help security researchers identify

Box 2.16 Independent audits of South African elections

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

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

Source: South Africa Electoral Commission

and remedy cybersecurity gaps.[116] The more salient threat to the election process is that the auditing process itself can be manipulated, in order to introduce doubts about the validity of the process, thereby prompting electoral disputes and potentially costly reruns.

Recommendation EMBs should develop regularly updated processes for auditing the use of election technologies, and consider how far these processes and their results can be made accessible to observers and the public.

Notes and references

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

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

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

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

5 Ellen Nakashima and Shane Harris (2018), 'How the Russians hacked the DNC and passed its emails to WikiLeaks', *The Washington Post*, 13 July, available at: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html

6 Matthew Cole, Richard Esposito, Sam Biddle and Ryan Grum (2017), 'Top-Secret NSA Report Details Hacking Effort Days Before 2016 Election', *The Intercept*, 5 June, available at: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/

7 Seda Gürses and Joris van Hoboken (2018), 'Privacy after the Agile Turn', in Evan Selinger and others (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press.

8 EU Foreign Affairs Council (2018), Council conclusions on malicious cyber activities, 16 April, Brussels, p.2, available at: http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf

9 See, generally, Vasilios Mavroudis and others (2017), 'A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components', in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (CCS '17), ACM, New York, NY.

10 Edgardo Cortés, Gowri Ramachandran, Liz Howard and Lawrence Norden (2019), *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials*, Brennan Center for Justice, p.8, available at: https://www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf

11 *McEwing and Kerr v Canada (Attorney General)* [2013] FC 525.

12 *R v Sona* [2014] ONCA 859; see, generally, Michael Pal (2017), 'Canadian Election Administration on Trial: "Robocalls", Opitz and Disputed Elections in the Courts', 28 *King's Law Journal* 324.

13 Michael Pal (2017), op. cit. endnote 1.
14 *WM Morrison Supermarkets Plc ('Morrisons') v Various Claimants* [2018] EWCA Civ 2339.
15 Canada Communications Security Establishment (2019), p.16, op. cit. endnote 1.
16 In 2018, for example, the Knox County Tennessee election night results reporting website was taken temporarily offline following a DDoS attack. No votes were tampered with, but the attack successfully caused concerns that the election had been compromised and that a larger attack was underway. See Center for Democracy and Technology (2018), *Election Cybersecurity 101 Field Guide – DDoS Attack Mitigation*, November, available at: https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/
17 Nic Cheeseman, Gabrielle Lynch and Justin Willis (2018), 'Digital dilemmas: the unintended consequences of election technology', *Democratization* 25(8), p.1398.
18 See, for example, Center for Internet Security (2018), *A Handbook for Elections Infrastructure Security*, February, p.15.
19 The Representation of the People (England and Wales) (Amendment) Regulations 2002, reg 106. See, generally, the Electoral Commission (2019), *Guidance for Electoral Registration Officers*, 'Part 4 – Maintaining the register throughout the year', Electoral Commission [UK].
20 Commonwealth Electoral Act [Australia] 1918.
21 Canada Elections Act (SC 2000, c. 9) s 101.
22 Election Act [Pakistan] 2017 s 79(3).
23 Such provisions may be provided for in overarching privacy and data protection law, in electoral law, or, in some cases, these data may be re-used by political parties and fall out of legal safeguards.
24 Jason Murdock (2016), 'Mexico election hack: Political party behind leak of 93.4 million voter records?', *International Business Times*, 25 April, available at: https://www.ibtimes.co.uk/mexico-election-hack-political-party-behind-leak-93-4-million-voter-records-1556608
25 'Hackeo masivo al padrón del INE', *El Universal*, 13 September 2017, available at: https://www.eluniversal.com.mx/nacion/politica/hackeo-masivo-al-padron-del-ine
26 Melissa Galván (2018), 'El INE denuncia la venta en internet de una copia de la lista de electores', *EXPANSIÓN politica*, 7 October, available at: https://politica.expansion.mx/mexico/2018/10/07/el-ine-denuncia-la-venta-en-internet-de-una-copia-de-la-lista-de-electores
27 Ibid.
28 UK Electoral Commission (2019), 'Modernising electoral registration: feasibility studies', available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/a-modern-electoral-register/modernising-electoral-registration-feasibility-studies
29 Centre of Excellence for CRVS Systems and the Global Partnership for Sustainable Development Data (2019), *A Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*, International Development Research Centre, p.118, available at: https://www.idrc.ca/en/news/compendium-good-practices-linking-civil-registration-and-vital-statistics-and-identity
30 American Civil Liberties Union (ACLU) (2018), 'Federal Court Blocks Indiana Voter Purge Crosscheck Law', ACLU, https://www.aclu.org/press-releases/federal-court-blocks-indiana-voter-purge-crosscheck-law (accessed 7 July 2019).
31 Nic Cheeseman and Brian Klaas (2019), *How to Rig an Election*, Yale University Press, New Haven, p.47.
32 UK Government, 'Register to Vote', available at: https://www.gov.uk/register-to-vote (accessed 4 November 2019).
33 See, generally, Information Commissioner's Office (2019), 'Update Report into Adtech and Real Time Bidding', 20 June.
34 Canada Communications Security Establishment (2019), op. cit., p.5

35 Catharine Tunney and Ashley Burke (2019), 'Federal parties being warned of efforts by 6 foreign countries to influence election: sources', CBC News, 16 September, available at: https://www.cbc.ca/news/politics/china-india-interference-1.5284473
36 National Cyber Security Centre (NCSC) (2019), Guidance for political parties, NCSC [UK], available at: https://www.ncsc.gov.uk/guidance/guidance-for-political-parties
37 National Cyber Security Centre (2019), Guidance for individuals in politics, NCSC [UK], available at: https://www.ncsc.gov.uk/guidance/guidance-for-individuals-in-politics
38 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/
39 Maciej Cegłowski (2019), 'What I Learned Trying To Secure Congressional Campaigns', *Idle Words*, 26 May, available at: https://idlewords.com/2019/05/what_i_learned_trying_to_secure_congressional_campaigns.htm
40 Alyza Sebenius and Kartikay Mehrotra (2020), 'Iowa Caucus Results Saved by Plain Old Paper After App Fails', Bloomberg News, 4 February, available at: https://www.bloomberg.com/news/articles/2020-02-04/iowa-caucus-results-saved-by-plain-old-paper-after-app-fails
41 However, research shows people are bad at matching individuals to photos. See, generally, Ross Anderson (2008), *Security Engineering* (2nd edn.), p.462.
42 Cortés et al. (2019), op. cit. endnote 10, pp.4–5.
43 The UK in 2019 conducted trials in ten local areas requiring different types of voter identification. See UK Cabinet Office (2018), 'Next round of Voter ID pilots announced for 2019', 3 November, available at: https://www.gov.uk/government/news/next-round-of-voter-id-pilots-announced-for-2019
44 UK Government (2019), 'The Queen's Speech 2019', 19 December, p.126, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_2019_-_background_briefing_notes.pdf
45 Source: Darryn van der Walt (2009), Port Elizabeth, following the fourth post-apartheid South African general election, Creative Commons Attribution licence, available at: https://www.flickr.com/photos/calico182/3465337579
46 UK Electoral Commission (2019), 'May 2019 voter identification pilot schemes', available at: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/our-research/voter-identification-pilots/may-2019-voter-identification-pilot-schemes
47 *The Economist* (2019), 'Britain plans to require that voters show photo ID', 17 October, available at: https://www.economist.com/britain/2019/10/17/britain-plans-to-require-that-voters-show-photo-id
48 Enrico Cantoni and Vincent Pons (2019), 'Strict ID Laws Don't Stop Voters: Evidence from a U.S. Nationwide Panel, 2008–2016', National Bureau of Economic Research Working Paper No. 25522, February.
49 Jacob R Neiheisel and Rich Horner (2019), 'Voter Identification Requirements and Aggregate Turnout in the U.S.: How Campaigns Offset the Costs of Turning Out When Voting Is Made More Difficult', *Election Law Journal: Rules, Politics, and Policy*, Vol. 18 No. 3.
50 Cheeseman and Klaas (2019), op. cit. endnote 32, ch.5.
51 Cheeseman et al. (2018), op. cit. endnote 17, p.1405.
52 Anna C Rader (2016), 'Politiques de la reconnaissance et de l'origine contrôlée: La construction du Somaliland à travers ses cartes d'électeurs' ['The Politics of Recognition and Authenticity: Constructing Somaliland through Voter Cards'], *Politique Africaine,* No. 144, pp.51–71 (translation by Google).
53 Gus Hosein and Carly Nyst (2014), 'Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries', I&N Working Paper 2014/1, p.21, available at: https://www.idrc.ca/sites/default/files/sp/Documents%20EN/WP2014-1-AidingSurveillance-web-Nov21.pdf
54 Ross Anderson (2008), Security Engineering (2nd edn.), p.478.

55 Miriam Golden, Eric Kramon and George Ofosu (2014), *Electoral Fraud and Biometric Identification Machine Failure in a Competitive Democracy,* v.2.5, 17 December, p.1, available at: https://columbiacpseminar.files.wordpress.com/2015/04/golden-kramon-ofosu.pdf
56 Cheeseman and Klaas (2019), op. cit. endnote 32, pp.67—68.
57 Madhavan Somanathan (2019), *India's electoral democracy: How EVMs curb electoral fraud*, Brookings Institution, 5 April, available at: https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/
58 PTI (2013), 'Supreme Court asks Election Commission to introduce paper trail in EVMs', *India Today*, 8 October, available at: https://www.indiatoday.in/india/north/story/supreme-court-asks-election-commission-to-introduce-paper-trail-in-evms-213615-2013-10-08
59 Dhananjay Mahapatra (2019), 'Count VVPAT slips of five booths in each assembly seat: SC', *The Times of India*, 9 April, available at: https://timesofindia.indiatimes.com/india/count-vvpat-slips-of-5-booths-in-each-assembly-seat-sc/articleshow/68786810.cms
60 Drew Desilver (2016), 'On Election Day, Most Voters Use Electronic or Optical-Scan Ballors', Pew Research Center, 8 November.
61 Eric Geller, Beatrice Jin, Jordyn Hermani and Michael B Farrell (2019), 'The scramble to secure America's voting machines', *Politico*, last updated 12 November 2019, available at: https://www.politico.com/interactives/2019/election-security-americas-voting-machines/
62 National Academies of Sciences, Engineering, and Medicine (2018), *Securing the Vote: Protecting American Democracy,* The National Academies Press, Washington, DC, pp.77–78, available at: https://doi.org/10.17226/25120
63 Cortés et al. (2019), op. cit. endnote 10, p.6.
64 Marie O'Halloran and Michael O'Regan (2010), 'E-voting machines to be disposed of', *The Irish Times*, 6 October, available at: https://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193
65 National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.80
66 National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.39, p.43: 'Research suggests that DRE VVPATs tend not to be voter verified. This suggests that VVPATs may be of little value as a check on the accuracy of DREs. See, for example, SP Everett, 'The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection', doctoral dissertation, Rice University, Houston, Texas; and Bryan A Campbell and Michael D Byrne (2009), 'Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability', *Proceedings of EVT/WOTE*, 2009.'
67 Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang and J Alex Halderman (2020), 'Can Voters Detect Malicious Manipulation of Ballot Marking Devices?', Proc. 41st IEEE Symposium on Security and Privacy, Oakland '20, San Francisco, May.
68 National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, p.79
69 Bundesverfassungsgericht, Docket Nos. 2 BvC 3/07 & 2 BvC 4/07, 2009. Translation by National Democratic Institute, available at: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany
70 Cheeseman et al. (2018), op. cit. endnote 17, p.1409.
71 Alexander J Martin (2018), 'Government rejects online voting for disabled voters amid electoral fraud fears', Sky News, 3 September, available at: https://news.sky.com/story/government-rejects-online-voting-for-disabled-voters-amid-electoral-fraud-fears-11489389
72 Royal National Institute of the Blind, 'Turned Out 2017', available at: https://www.rnib.org.uk/sites/default/files/Turned%20Out%202017%20APDF_1_0.pdf
73 Andrew Ellis, Carlos Navarro, Isabel Morales, Maria Gratschew and Nadja Braun (2007), *Voting from Abroad: The International IDEA Handbook*, Handbook Series, International Institute for Democracy and Electoral Assistance, 26.

74 More information is available on the website of the Election Commissioner of India, available at: https://eci.gov.in/divisions-of-eci/it-applications-etpbs-servicevoter/
75 Swiss Info (2019), 'Three cantons seek damages for failed e-voting system', 8 July, available at: https://www.swissinfo.ch/eng/swiss-post_three-cantons-seek-damages-for-failed-e-voting-system/45083860
76 Bart Jacobs and Wolter Pieters (2009), 'Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment', in Alessandro Aldini, Gilles Barthe and Roberto Gorrieri (eds.), *Foundations of Security Analysis and Design V,* Springer Berlin Heidelberg, Vol. 5705 DOI: 10/dk7qdp; G Schryen and E Rich (2009), 'Security in Large-Scale Internet Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland', 4(4), IEEE Transactions on Information Forensics and Security 729 DOI: 10/dr9676.
77 Estonian National Electoral Committee and the State Electoral Office (2019), 'Statistics about Internet voting in Estonia', available at: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia (accessed 22 July 2019).
78 National Academies of Sciences, Engineering, and Medicine (2018), op. cit. 63, pp.101–106.
79 See *Ch. Nasir Iqbal and others v Federation of Pakistan thr. Secy. Law and others* (PLD 2014 SC 72).
80 *Miss Yasmin Khan and another v Election Commission of Pakistan, Islamabad through Secretary and another* (1994 SCMR 113).
81 *Ch. Nasir Iqbal and others v Federation of Pakistan through Secretary Law and others* (Const. P. 39/2011); *Imran Khan, Chairman, PTI, etc. v Federation of Pakistan* (Const. P. 90/2011).
82 Elections Act (Pakistan) 2017, s 94.
83 Election Commission of Pakistan (2019), *Report on I-Voting Pilot Test in 35 Constituencies Held on 14th October 2018,* Election Commission of Pakistan, Islamabad, p.5.
84 Elections Act 2017, s 94.
85 See *Farhat Javed Siddique and others v Government of Pakistan* (Const. P. 74-79/2015, 49-56/2016, 2/2018, Civil Misc. Apps. 4292/2017, 162/2018); Elections Act 2017, s 239.
86 ECP Notification S.R.O. 1166(I), 28th September 2018.
87 Elections Act 2017, s 69.
88 Calculated by one of the authors from electoral data as an illustrative indication, following discussion in interviews with officials – do not cite as an official statistic.
89 See, generally, NADRA, 'International Projects', available at: https://www.nadra.gov.pk/international-projects/.
90 ECP Order of April 19, 2018 (F No 6(1)/2011-IT), p.3.
91 Internet Voting Task Force (IVTF) (2018), *Findings and Assessment Report of Internet Voting Task Force (IVTF) on Voting Rights of Overseas Pakistanis*, Election Commission of Pakistan, Islamabad.
92 ECP Order of April 19, 2018 (F No 6(1)/2011-IT).
93 Elections Act 2017, s 94; Constitution of Pakistan, art 226.
94 See https://www.youtube.com/watch?v=iFpmUaefD34 and https://www.youtube.com/watch?v=7JWEaHCg4ns for the English versions.
95 Election Commission of Pakistan (2019), op. cit. endnote 84.
96 Survey.
97 Interview with OSCE/ODIHR Long-Term Observer, Alex Folkes, 13 November 2019.
98 Many of these tweets can be read by searching for the hashtag #IDOX (last accessed 3 January 2019).
99 Jim Waterson, Hilary Osborne and agencies (2019), 'BBC denies Laura Kuenssberg's postal vote comments broke law', *The Guardian*, 11 December, available at: https://www.theguardian.com/media/2019/dec/11/bbc-denies-political-editors-postal-vote-comments-broke-law
100 Center for Internet Security (CIS) (2018), *A Handbook for elections infrastructure security*, February, p.29, available at: https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

101 Cheeseman and Klaas (2019), op. cit. endnote 32, pp.177–179.
102 Brown and Lee (March 2019), Interviews with the Electoral Commission of Ghana.
103 Cheeseman et al. (2018), op. cit. endnote 17, pp.1405–1406.
104 Ibid, p.1407.
105 HM Treasury (2015), *The Aqua Book: Guidance on Producing Quality Analysis for Government,* HM Government.
106 Brown and Veale (March 2019), Interviews with the Electoral Commission of Pakistan.
107 Luke Tyburski (2019), 'Malawi's Election Was Not Stolen With White-Out', *Foreign Policy*, 1 November, available at: https://foreignpolicy.com/2019/11/01/malawis-election-was-not-stolen-with-white-out/
108 Cheeseman et al. (2018), op. cit. endnote 17, p.1408.
109 Andy Greenberg (2017), 'Everything We Know About Russia's Election-Hacking Playbook', 8 June, available at: https://www.wired.com/story/russia-election-hacking-playbook/
110 BBC News (2017), 'Venezuela vote: Turnout figure "tampered with"', 2 August, available at: https://www.bbc.co.uk/news/world-latin-america-40804812
111 Girish Gupta (2017), 'Exclusive: Venezuelan vote data casts doubt on turnout at Sunday poll', Reuters, 2 August, available at: https://www.reuters.com/article/us-venezuela-politics-vote-exclusive-idUSKBN1AI0AL
112 Tom Wilson, David Blood and David Pilling (2019), 'Congo voting data reveal huge fraud in poll to replace Kabila', *Financial Times*, 15 January, available at: https://www.ft.com/content/2b97f6e6-189d-11e9-b93e-f4351a53f1c3
113 Tom Calverley (2020), 'Congolese torture survivor gets Home Office reprieve', *The Guardian*, 15 January, available at: https://www.theguardian.com/politics/2020/jan/15/congolese-torture-survivor-gets-home-office-reprieve
114 IDEA (2015), op. cit. endnote 4, p.19.
115 Cheeseman and Klaas (2019), op. cit. endnote 32, p.237.
116 IDEA (2015), op. cit. endnote 4, p.46