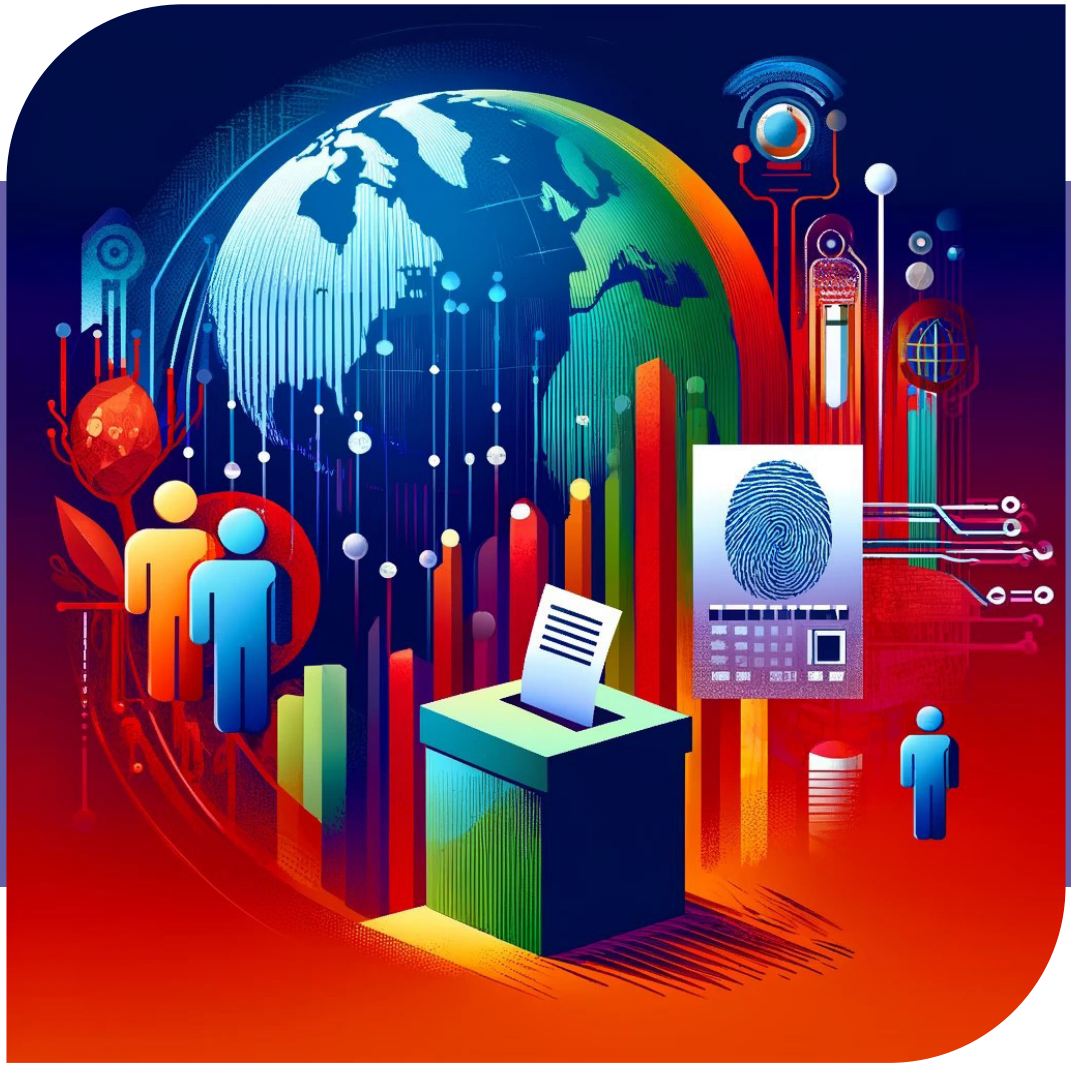
International IDEA

ARTIFICIAL INTELLIGENCE FOR ELECTORAL MANAGEMENT



ARTIFICIAL INTELLIGENCE FOR ELECTORAL MANAGEMENT

Prathm Juneja

International IDEA
INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

Cover illustration: Generated with DALL E
Design and layout: International IDEA
Copyeditor: Curtis Budden

DOI: <https://doi.org/10.31752/idea.2024.31>

ISBN: 978-91-7671-764-6 (PDF)

Contents

Abbreviations

AI	Artificial intelligence
CCTV	Closed-circuit television
EMB	Electoral management body
GDPR	EU General Data Protection Law
GenAI	Generative artificial intelligence
LLM	Large language model
OCR	Optical character recognition
OMR	Optical mark recognition

EXECUTIVE SUMMARY

EMBs have to develop plans to respond to and, in some cases, use AI to maintain free, fair and secure elections.

As artificial intelligence (AI), including its potential role in influencing elections, has become an increasingly important topic, electoral management bodies (EMBs) have to develop plans to respond to and, in some cases, use AI to maintain free, fair and secure elections. AI is a rapidly evolving category of technologies that are largely unregulated, and very little research has been conducted so far concerning its potential impact on elections.

This Report is aimed at supporting EMBs and other relevant parties in developing a broad understanding of the opportunities, challenges and legal implications of the use of AI for elections. It has two main areas of focus. First, it offers a starting point to examine some of the ways in which EMBs may be able to use AI to improve the administration of elections; it presents the risks and potential mitigation strategies associated with those use cases. Second, it covers some of the ways that other, non-EMB actors may use AI to impact election processes as well as potential strategies for EMBs to respond. It describes some of the regulatory frameworks for AI starting to take shape around the world, and explains how they may impact the work of EMBs that are considering using, and responding to other actors' use of, AI as a part of the electoral process.

As EMBs' use of AI is still nascent, this Report looks at the limited examples of, and scholarly work on, the subject and combines them with insights from various industries and other academic fields to highlight potential areas for AI use in the pre-electoral, electoral and post-electoral stages of the electoral cycle, as well as the use of generalist generative AI tools, such as ChatGPT, for EMB

staffers. These use cases include AI for voter list management, voter registration, resource allocation planning, forecasting election costs, targeted advertising, campaign monitoring, biometrics and voter verification, ballot counting and post-electoral audits. Every case raises a series of ethical, human rights and practical concerns, such as issues of surveillance, bias, discrimination, accuracy, performance, technical capabilities, cybersecurity and public trust. In many of these cases, EMBs considering the use of AI may be able to mitigate these concerns through careful human oversight, testing and auditing of AI systems.

This Report does not take a stance on whether EMBs should consider the use of AI for elections; rather, it offers an introduction to the subject for EMBs considering these use cases, as well as recommendations for developing clear, transparent and rights-respecting rules for implementation.

The Report covers the oft-discussed issue of AI use by other political actors, including misinformation producers, political campaigns and hackers. Although misinformation about elections is not a new phenomenon, advances in generative AI exacerbate existing problems by increasing the quantity and, in some cases, improving the quality of misinformation. Ensuring transparency, engaging in interagency cooperation and developing partnerships with the providers and disseminators of AI-generated content are potential mitigation strategies for this concern.

Political campaigns are likely to use AI for everything from targeted advertising to election forecasting, and EMBs should consider how these use cases may require updates to their mandate and regulations. AI may also increase the threat of cyberattacks, especially through higher-quality phishing attempts, and EMBs should consider strengthening existing cybersecurity protocols to defend against these advances in capability.

Political campaigns are likely to use AI for everything from targeted advertising to election forecasting.

A rapidly developing regulatory environment may also influence the role of AI in elections. In this Report we offer a brief introduction to a few regulatory approaches to AI, including the European Union's Artificial Intelligence Act—and its focus on high-risk systems—as well as the United States' Artificial Intelligence Executive Order and

Brazil's Superior Electoral Court regulations. In all three cases, these regulations impact the ways EMBs may be able to use AI for their own work, and they may impact EMBs' mandates, especially as they pertain to monitoring political campaigns.

It is increasingly important for EMBs to start developing plans to adapt to the new technological environment.

While there is still much uncertainty about how EMBs may use AI, as well as how other actors' uses of AI will impact elections, it is increasingly important for EMBs to start developing plans to adapt to this new technological environment. This Report offers a starting point for that work by offering a broad overview of AI for elections, including the opportunities, challenges and mitigation strategies associated with its use by both EMBs and other relevant actors.

INTRODUCTION

Artificial intelligence (AI) is an increasingly relevant topic for electoral management bodies (EMBs) and other organizations involved in electoral processes. In general, much of the conversation around AI and elections has focused on the role that AI may play in the generation and dissemination of misinformation.[1] While this is an important topic, covered in multiple parts of this Report, the potential role and impact of AI on elections is a much broader subject, encompassing everything from how EMBs may consider implementing AI as a part of electoral processes to the ways that other political actors could use AI to influence elections.

Much of the conversation around AI and elections has focused on the role that AI may play in the generation and dissemination of misinformation.

To begin to fill in this gap, this Report offers a framework for EMBs considering the use and impact of AI for elections and electoral management. As AI and elections is a broad, rapidly developing topic, this Report highlights potential areas for further exploration for EMBs beginning to develop AI strategies for their specific contexts.

Although research on the topic of AI for electoral management is still scant, the primary goal of this Report is to offer EMBs a starting point—by drawing on examples from other fields as well as looking at existing processes within EMBs—for examining how the use of AI may help improve the administration of elections. A disproportionate number of examples of EMBs' current use of AI included in this Report come from the United States, which has had many opportunities to use AI due to its federalized electoral system,

1 As defined by the UNHCR (2022), misinformation is false or inaccurate information that is shared, and includes disinformation, which is deliberately sharing misinformation, including malicious content such as hoaxes, spear phishing, or propaganda.

often run at a state and county level, as well as the sizeable number of AI companies operating in the country.

Advances in AI have created opportunities for EMBs.

Advances in AI have created opportunities for EMBs to deploy systems with better reasoning as well as analytical and generative capabilities with the potential to increase accessibility to, optimize logistical planning for, and improve the information environment around, elections. These potential benefits come with possible negative externalities around cybersecurity, human rights, discrimination and other issues.

It is worth noting that this Report is not meant to explicitly recommend, or offer implementation instructions for, the use of AI by EMBs; rather, it offers a broad introduction for EMBs interested in the topic. Another goal of the Report is to provide EMBs with a starting point for examining how other actors, such as political campaigns and hackers, may use AI to influence the management and outcome of elections. Given the proliferation of, and ease-of-access to, advanced AI tools, EMBs must begin to plan for these uses of AI, including the implementation of mitigation strategies and the development of regulatory approaches.

The Report is organized as follows. In Chapter 1 we offer a definition of AI and some historical context for its use in elections, and we discuss how recent advances in AI motivate this Report. In Chapter 2 we provide a non-comprehensive list of possible AI use cases for EMBs across the electoral cycle, including steps towards implementation, concerns associated with the use cases and potential mitigations for some of these concerns. In Chapter 3 we discuss a distinct but relevant area for EMBs—how other political actors may use AI to influence electoral management—and what EMBs should begin to prepare for in the short term. Finally, in Chapter 4, we discuss some of the global and country-specific approaches to regulating the use of AI, especially for public bodies, and how these regulations may shape EMBs' use of, and response to, AI.

Chapter 1

SETTING THE SCENE: AI AND ELECTIONS

1.1. DEFINING AI

For this Report, we rely on the widely accepted definition of AI systems provided by the Organisation for Economic Co-operation and Development (2019):

> An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Traditional statistical methods, such as linear regressions and probabilistic pattern matching, as well as modern machine learning techniques, such as neural networks, are all covered under this definition if they are used to develop outputs that could influence physical or virtual environments. Based on this definition, we use the term AI in this Report to cover a breadth of systems, and we use more specific terms to describe underlying technologies. For more information on terms, review Annex A: Key terms.

1.2. **AI ADVANCES AND USE IN ELECTIONS**

AI has long been used as a part of electoral management efforts. In the USA, for example, the Electronic Registration Information Center (ERIC) works with a consortium of states to analyse voter registration, motor vehicle and other official records to assist with voter roll maintenance. ERIC's software is machine learning–based, offering recommendations to state electoral officials on voters who are likely to have been registered twice and on eligible unregistered voters (Electronic Registration Information Center 2024). Biometric verification systems, in use or under trial in many countries, are often examples of AI that use deep learning models to match biometric data to existing data sets (Wolf et al. 2017). Signature matching tools, also widely used in the USA, are an example of AI (Bender 2022). Countries using statistical modelling techniques for resource allocation, polling site placement, advertising campaigns or election results analysis may also be using varying forms of AI.

Although rarely acknowledged as such, AI is not new to elections or election administrators. Advances in the development, deployment and marketing of AI, however, have increased both the opportunities for, and trade-offs from, its use in elections.

The earliest research into what we now consider AI likely began sometime in the early to mid-20th century, with the Turing test and early conceptions of artificial neural networks. Early progress in AI focused mostly on the narrow task of designing so-called expert systems, or models trained to mimic human experts in specific domains, with many early AI developments concentrating on decision making for games. Until recently most progress in AI pertained more to these narrower systems, with models operating more akin to traditional statistics, taking specific inputs and developing interpretable formulas for how they result in outputs, than to the abstractions we associate with deep learning approaches.

The current AI era has been driven largely by advances in deep learning, including transformer architecture (Vaswani et al. 2017). These innovations, alongside the increasing availability of large data sets and computational processing power, have made it possible for deep learning models to take in large swathes of unstructured

data, including text, images and video, and to use those data to train generalized models. Advances in transfer learning have enabled developers to specialize these larger models for various domains, including medicine, science, media and, increasingly, politics. Although deep learning approaches have drastically improved performance in many tasks, especially in the modelling of languages, they often come with the trade-off of a lack of interpretability, owing to the levels of abstraction inherent in deep neural networks. Whereas traditional regressions offer clear formulas for how inputs are turned into outputs, deep neural networks obscure how and why specific inputs result in specific outputs.

It is these more recent advances that motivated this Report and that are creating new opportunities and concerns for electoral authorities. Large language models (LLMs) offer EMBs and political actors the ability to analyse, generate and summarize complex text. Other generative AI (GenAI) models offer similar capabilities for other types of output, including video, audio and numerical data. Advances in techniques such as graph neural networks and boosting and bagging methods open up new avenues for the analysis of networks and complex data sets. In the following section, we discuss some ways EMBs may be able to use AI systems to improve the administration of elections. Later, we discuss the ways other actors' use of AI is likely to impact EMBs.

It is worth noting that government agencies and corporations around the world are already running trials involving many of these advances in AI in various forms, and many countries are in the process of establishing guidelines for the use of AI (Carrasco et al. 2024). These broader public sector AI strategies are likely to impact the resources and capabilities EMBs will have access to in any implementation of AI for electoral management.

Many countries are in the process of establishing guidelines for the use of AI.

Voter registration and identification

AI use case. A goal of the voter registration process is to pre-verify a person's eligibility to vote so that, when a voter submits their ballot, only their identity needs to be verified. In jurisdictions where active voter registration is required, this process often requires that voters present some form of official identification, proof of eligibility and possibly biometric data, such as fingerprints, facial images or a signature. AI models trained on matching identification documents or biometric details can speed up, and potentially improve the accuracy of, this process and prevent duplicate registration. AI offers new forms of biometric voter identification at polling stations, such as facial identification and thumbprinting, where a model can compare a voter's biometrics against the biometric data included on the voter register.

Implementation. In many cases biometric tools are AI-based, using deep learning models to match biometric hashes (i.e. numerical representations of biometric data such as fingerprints). The use of a biometric system for voter registration offers EMBs an opportunity to either reverify biometric data at polling sites or include it on voter ID cards. As of 2016, 35 per cent of surveyed EMBs were capturing biometric data as a part of their registration process (Wolf et al. 2017). India, which has a general biometric ID system that includes iris, fingerprint and facial data, is exploring the use of these data for voter identification (Livemint 2022).

Concerns. It is worth noting that in jurisdictions where voter fraud is extremely uncommon, strict verification methods may do little to improve election security while wrongfully disenfranchising legitimate voters (Padmanabhan, Simoes and MacCarthaigh 2023). The accuracy of signature matching tools may be as low as 74.3 per cent, which could lead to the disenfranchisement of eligible voters (Hussain et al. 2015). Although failure rates for biometric systems are often low, when they do fail, they may fail disproportionately for people of colour and result in discriminatory disenfranchisement (Padmanabhan, Simoes and MacCarthaigh 2023; Wolf et al. 2017). Biometrics present serious data security and privacy concerns, which, apart from being issues themselves, may dissuade privacy-conscious or historically targeted voters from participating in elections (Wolf et al. 2017). EMBs may mitigate some of these concerns by offering

alternatives to biometric pre-verification as well as creating clear, easily accessible processes for appealing decisions relating to biometric systems.

2.2.2. **Planning**

AI models and simulations may be useful in optimizing the pre-election planning process.

Polling site locations and resource allocation

AI use case. A key aspect of the pre-election planning process is deciding where to allocate electoral resources, such as the location of polling sites, the number of polling booths and the number of election workers at specific polling sites. Accurate estimates of where resources may be required make election processes more accessible, faster and easier for voters. AI models and simulations may be useful in optimizing this process and, in some cases, making it more objective by predicting the popularity of polling places and minimizing the distance between voters and their polling sites. Similarly, models may be useful for estimating where election workers may be most necessary. The use of such models could potentially improve access to polling sites, with potential impacts on voter turnout rates.

Implementation. As Padmanabhan, Simoes and MacCarthaigh (2023) note, although there is little evidence that AI is being used to select polling site locations, work is being carried out in other industries that use AI to optimize the location of facilities (Al-Haidary et al. 2021). AI-based employee scheduling/allocation tools may be useful for allocating workers at different polling sites (Talarico and Maya Duque 2015). Internally built models for these purposes may use supervised algorithms, trained on 'ideal' scenarios for polling sites and resource allocation based on historical data, or unsupervised algorithms, aimed at optimizing distance or efficiency.

Concerns. A lack of nuance in the data available for models presents a serious concern with the use of AI to select the location of polling places (e.g. whereas an election official may understand perceptions of the accessibility or safety of a specific location, models may miss this nuance). Data sets may also miss information about accessibility, community importance, visibility and interior quality, some of which have been shown to impact turnout rates (Mann and Stein 2019). Algorithms aimed at constantly optimizing polling

site locations may increase the cost of communicating about new locations, and volatility could confuse voters, potentially decreasing turnout rates (Padmanabhan, Simoes and MacCarthaigh 2023). Although important, human oversight may be difficult here, too, as manual changes, such as moving a polling location, could impact the model's calculations, further complicating its objectivity. Optimizing for specific variables, such as general distance from a polling place, could result in discrimination against certain categories of voters, such as rural voters. Similar serious concerns arise for general resource allocation, in terms both of polling booths and of election workers (Kwon, Moreno and Raman 2023).

Baseline estimation setting

AI use case. In some cases, and depending on its mandate, an EMB may want to develop a set of expectations of various election outcomes, including campaign fundraising, campaign expenditures, voter turnout rates and even election results. In all cases these estimates may serve as a useful baseline for detecting anomalies during or after an election. For example, predictions of campaign fundraising may enable EMBs to better monitor campaign spending, audit requests and media purchases. Predictions of voter turnout rates may enable EMBs to better prepare for logistical needs, such as the allocation of ballots before an election and the counting of ballots after one. Traditional statistical techniques, such as regressions, and more advanced AI models may be useful for these processes.

Implementation. Perhaps the most important baseline estimation that may be useful for other areas of EMBs' work is using AI or data science techniques to predict potential voter turnout rates. EMBs could consider traditional methods used by academics and polling agencies for this or more advanced methods, such as random forest or boosting methods (Moses and Box-Steffensmeier 2021; Kennedy, Wojcik and Lazer 2017). Similar methods may be useful for predicting campaign expenditures and fundraising trends, with some research examining methods for similar tasks in the investing, crowdfunding and non-profit spaces (Liu and Hu 2024). There has been an increase in the number of political start-ups seeking to sell machine learning tools that provide turnout and fundraising predictions to political campaigns (Markay 2022). Substantial differences in actual results and estimated results may be useful as flags for further investigation.

Concerns. The major concern with the use of AI for baseline estimation is the high likelihood of inaccurate results from modelling techniques. Voter turnout and campaign fundraising statistics are influenced by diverse factors, many of which go unmeasured. AI and traditional statistical methods are unlikely to offer sufficiently reliable estimates to be useful for EMBs to make good decisions or to be used as a baseline for comparison except in situations where predictions differ drastically from reality. Inaccuracy could impact EMBs' decision making and fairness in the auditing process. EMBs' use of predictions in any form could be problematic for electoral integrity. These models pose a significant risk in terms of electoral integrity, campaign activities and public trust if they are leaked. EMBs considering implementing AI for these purposes may be able to mitigate these concerns with stringent cybersecurity practices and thorough piloting and comparison of new models to test their reliability.

Forecasting election costs

AI use case. It may be useful for EMBs to forecast the administrative cost of an election as a part of their budgeting process. Since elections have many variable costs, ranging from purchasing polling machines and ballots to hiring election workers, AI may be useful in improving estimates of necessary equipment, people and other resources. Many EMBs already engage in rough forecasting for budgeting purposes, often basing estimates on the worst-case scenario of previous elections, but AI may offer more accurate estimates. Like with resource allocation and baseline estimation setting, AI models may offer rough predictions of various costs, such as for election security, polling machines, employees, paper ballots and others.

It may be useful for EMBs to forecast the administrative cost of an election as a part of their budgeting process.

Implementation. Limited research has been conducted on the costs of electoral management, and we were unable to find any work that uses AI (Clark 2019). However, some research has examined the role deep learning algorithms can play in assisting with government budgeting strategies, generally by using potential expenditures as inputs to optimize specific outputs (Valle-Cruz, Fernandez-Cortez and Gil-Garcia 2022). Advances in using machine learning in the fields of risk prediction and insurance pricing may serve as a useful starting point (Kan et al. 2019).

Concerns. Given the lack of research examining methods for predicting election costs, the major concern with the use of AI for this purpose is accuracy. The risk of low-accuracy models, especially those relied on to make decisions, is that EMBs may be underprepared for elections, which could have serious consequences for electoral integrity. EMBs may be able to mitigate these concerns by piloting AI-based forecasts and testing their accuracy compared with existing methods.

LLMs may be useful in detecting social media posts about planned or potential violence at different polling locations.

Electoral security/violence prediction

AI use case. In order to maintain election security and integrity, EMBs and security agencies may benefit from predictions of sites where electoral violence could potentially occur. Much like in the previous sections, models trained on areas where violence has occurred previously or areas with other correlates of violence may help EMBs decide where to prioritize security services. Additionally, LLMs may be useful in detecting social media posts about planned or potential violence at different polling locations. Combined, these models may enable EMBs to predict high-risk polling locations and prevent violence from occurring.

Implementation. Supervised models trained on polling sites or geographies with previous electoral violence issues may be useful for predicting where future events will occur (Padmanabhan, Simoes and MacCarthaigh 2023). Fine-tuned LLMs run on social media posts may be useful for flagging potential threats of violence or may be able to highlight specific areas receiving disproportionate attention from violent groups. Although there is limited work on polling sites in particular, AI has long been used for predictive policing, with many governments and private companies developing tools for the purpose (Hardyns and Rummens 2018).

Concerns. Predictive policing efforts are highly controversial, with serious ethical and human rights concerns around accuracy and discrimination. Due to the lack of high-quality data, existing biases and the uninterpretability of most deep learning algorithms, there is evidence that these systems perpetuate systemic inequities in policing without strong evidence of effectiveness (Gstrein, Bunnik and Zwitter 2019; Richardson, Schultz and Crawford 2019). There is little evidence of predictive policing resulting in effective outcomes,

but there is a lot of work describing its potential to exacerbate civil and human rights violations (Van Brakel 2016). Increasing policing at polling sites may suppress voter turnout rates, impact electoral outcomes and reduce trust in the process (Padmanabhan, Simoes and MacCarthaigh 2023).

2.2.3. **Civic education and voter mobilization**

Sharing election information

AI use case. AI, especially LLMs, may be useful for the purposes of tailoring election information to specific subsets of the population. As many EMBs have a mandate to increase equity and access in voting, using diverse communication strategies for different subsets of the population may be one way to ensure equal access to information. This is especially pertinent for voters with limited technical knowledge, as AI may be used to develop ways to present election information that can be understood more intuitively. For example, LLM-based chatbots trained on EMB information and frequently asked questions may serve as a useful way for EMBs to offer existing information in a format tailored to voters' specific questions that is easier to use than navigating election websites manually (Eisen et al. 2023).

Implementation. Some research has developed a chatbot architecture for improving access to election information for senior citizens and first-time voters; the chatbot is trained specifically on frequently asked questions from EMBs (Muppasani et al. 2023). EMBs must be careful when using chatbots, making sure to use closed-loop technologies such as retrieval augmented generation to make sure the LLM uses only predefined information to answer queries.

Concerns. The use of LLM chatbots for electoral management poses serious concerns about information validity; EMBs will have to carry out extensive testing and auditing to prevent LLM hallucinations and the spread of false information (Rawte, Sheth and Das 2023). Security audits are necessary given the ability of nefarious actors to 'jailbreak' or exploit LLMs to leak data or provide incorrect information (Wei, Haghtalab and Steinhardt 2023). Even with a low likelihood of errors, any false information shared by an EMB-sanctioned chatbot is likely

to cause controversy and issues with electoral integrity. EMBs may be able to mitigate these concerns with extensive testing and auditing, as well as by using models with limited hallucination probabilities.

EMBs with a mandate to increase voter turnout rates or distribute election information to diverse populations may benefit from the use of AI to create targeted advertising campaigns.

Targeted advertising

AI use case. EMBs with a mandate to increase voter turnout rates or distribute election information to diverse populations may benefit from the use of AI to create targeted advertising campaigns. Targeted advertising may be useful in increasing access to information for people not normally engaged in election processes. GenAI models may be able to automate the process of creating, or developing the first draft of, advertising for small groups of the population. AI, especially unsupervised models, such as clustering models, may be useful for the process of identifying groups that have been historically neglected in EMB communications.

Implementation. Most work on the role of GenAI for voter mobilization focuses on the role it may play in targeted political advertising on the part of campaigns and affiliated organizations. Some work finds that using GenAI tools to modify ads according to users' personality traits saw increases in engagement (Simchon, Edwards and Lewandowsky 2024). Earlier work studying microtargeted ads on Facebook found an impact on turnout rates only in highly competitive US elections (Haenschen 2022). Implementation would require feeding data about users (generally from social media companies) into GenAI tools to generate targeted advertising for subsets of the user base.

Concerns. Microtargeting, especially driven by GenAI, raises serious concerns regarding data privacy, manipulation and accuracy. Voters may be uncomfortable with the use of their personal data for the purposes of 'nudging' them to vote, and successful interventions risk creating inequities in the election process and potentially calling electoral integrity into question. Fully automated systems may result in GenAI tools hallucinating, sharing incorrect information about elections or being politically biased. Additionally, both the process of selecting groups to microtarget and the platforms used to deliver those advertisements raise concerns about creating inequities, as EMBs may disproportionately advertise to certain subgroups of the population (Ali et al. 2019). The potential usefulness of these tools is

still under-researched, and they may not have any meaningful impact on turnout rates when compared with more general voter mobilization strategies, which may result in proportionality concerns.

2.3. **ELECTORAL PERIOD**

The electoral period is the portion of the electoral cycle where the focus is largely on campaigning, voting, monitoring and tabulating results.

2.3.1. **Campaign and media monitoring**

Monitoring misinformation on social media

AI use case. One potential AI use case for EMBs is the use of LLMs and graph neural networks on social media platforms to detect and summarize common misinformation regarding elections. LLMs may be able to detect trends in misinformation and flag the most concerning cases, such as categories of posts with misleading information about the time or location of an election or about the eligibility of particular voters. Models may also be useful for detecting specific posts that violate election laws. This may offer EMBs an opportunity to develop plans to respond faster and with more ease than manually monitoring social media platforms, key elements in reducing the impact of misinformation on elections. The threat of election-related misinformation on social media is further discussed in Chapter 3.

Implementation. A sizeable amount of research has examined the use of LLMs to detect or summarize misinformation trends, and a variety of private companies and non-profits are building tools for this task (Kondamudi et al. 2023; Dhiman et al. 2023). Implementation of these tools will require careful planning to include information about the specific context of an election, training for languages spoken in the jurisdiction of interest, the identification of key platforms where misinformation is spread and the incorporation of human observers. Partnerships with platforms, fact-checking organizations and other third parties may prove useful for accessing, removing and responding to misinformation about elections.

Concerns. An overreliance on AI for misinformation detection could result in EMBs missing key topics and concerns, especially on private messaging platforms (e.g. WhatsApp), where data availability is limited. Most LLMs are optimized predominantly for the English language, and often for the US context, which could cause models to miss important details. The performance of detecting misinformation requires a clear understanding of what constitutes misinformation and of the legality of policing or responding to it. EMBs may be able to mitigate these concerns by using AI only as one part of a broader misinformation strategy. Questions of free speech, surveillance and government monitoring of public platforms may arise, especially as they pertain to human rights and the freedom of expression (Inter-American Commission on Human Rights 2017).

Campaign and media monitoring

AI use case. In many jurisdictions EMBs are responsible for monitoring the content and timing of communications from campaigns, other political groups and media organizations. For example, some countries have a mandated campaign silence period prior to voting, which AI may help detect violations of. Fine-tuned LLMs with social media and Internet data streams may be helpful for flagging specific content that goes against EMB guidelines, similar to the process described for detecting misinformation.

Implementation. Implementation for this task will be more bespoke than for detecting misinformation, as limited work has been done on the subject. LLMs may be fine-tuned on data sets of content that is 'permitted' and 'not permitted' and then fed inputs from the social media accounts of political campaigns and media organizations to flag them for potential violations.

Concerns. As in the case with the detection of misinformation, a serious concern arises with an overreliance on AI-based tools for this purpose, as they are likely to miss potential violations. Additionally, models may perform in a discriminatory manner, finding more violations from, for example, one political party due to poorly designed training data. This could result in discriminatory consequences if not balanced by other forms of observation. To mitigate some of these concerns, EMBs considering implementing

this use case should consider using it as one piece of a broader media monitoring strategy.

2.3.2. **Voting operations**

Voter identification documents

AI use case. AI models may be useful for verifying voter identification documents. Many EMBs and governments already use technological tools for scanning and comparing identification documents against existing databases, and AI may improve the accuracy of these technologies. Models may enable election officials to verify that a voter's address is within the bounds for the polling site.

Implementation. As many EMBs already use existing hardware and software tools for the verification of identification documents, AI implementation may involve updating the models used for scanning and verifying documents. Supervised models, trained on legitimate and illegitimate identification documents, are likely to be the most useful for this task. AI-based optical character/mark recognition (OCR/OMR) tools may be useful for scanning and querying non-standard forms of identification.

Concerns. In many cases identity verification tools rely on scanning barcodes, magnetic strips or secure chips on or inside identification documents and cards. These approaches are likely to perform better than AI models, as they do not rely on inference or predictions. AI models may be less accurate compared with traditional forms of identity verification. It is worth noting that in countries with low rates of voter fraud or low rates of identification ownership, a voter identification requirement is likely to disenfranchise voters without impacting the security of elections (Hajnal, Kuk and Lajevardi 2018).

Biometrics and voter verification

AI use case. As mentioned in 2.2.1: Voter registration and eligibility, AI models may be useful for countries using biometric (e.g. eye, face, palm, thumbprint) recognition for voter verification. A model can compare the biometrics of a person submitted during registration or during other official processes with the biometrics of a person submitting a ballot. This may enable voter authentication without identification documents and could improve the security of elections.

AI models may be useful for countries using biometric recognition for voter verification.

Implementation. Implementation for this task is a two-step process: first designing a system to capture biometric information during the registration process (see 2.2.1: Voter registration and eligibility) and second, verifying those biometrics at the polling site. This part of the process is where AI is most likely to be used, with deep learning models being used to match biometric hashes. These models are likely to be developed by external vendors, as they require large training data sets that EMBs are unlikely to have the capacity to build themselves. As mentioned earlier, as of 2016, 35 per cent of surveyed EMBs were capturing biometric data during the registration process (Wolf et al. 2017). And some countries, including India, are piloting the use of these data for voter identification (Livemint 2022). AI-based signature matching tools are used regularly in elections, with at least 29 of the largest US counties using them to verify mail-in ballots (Bender 2022).

Concerns. As mentioned in 2.2.1: Voter registration and eligibility, voter fraud is extremely uncommon in many jurisdictions, and verification methods may result in much more harm than good depending on a country's specific circumstances (Padmanabhan, Simoes and MacCarthaigh 2023). Additionally, the accuracy of signature matching tools may be as low as 74.3 per cent, which could lead to the disenfranchisement of eligible voters (Hussain et al. 2015). Although failure rates for biometric systems are often low, when they do fail, they may fail disproportionately for people of colour and result in discriminatory disenfranchisement (Padmanabhan, Simoes and MacCarthaigh 2023; Wolf et al. 2017). Biometric systems present serious concerns around data security, privacy, and human rights, potentially dissuading people from participating in electoral processes. This raises questions of proportionality: do the associated security risks, potential human rights concerns, and disenfranchisement probabilities outweigh the advantages of biometric identification?

2.3.3. **Polling place monitoring**

Detecting polling place incidents

AI use case. Over the past few years, voters have frequently posted complaints on social media platforms about issues with elections and at polling places. These may include reports of non-functioning

machines, long lines, voter suppression or illegal behaviour. LLMs can be used to monitor social media platforms for these complaints, automatically categorize them and forward them to the appropriate authorities.

Implementation. There is evidence that fine-tuned LLMs can detect reports of polling place incidents in US elections with a high degree of accuracy (Juneja and Floridi 2023). Implementation requires access to social media data, most likely through partnerships with platforms, for specific election-related keywords and the creation of labelled data sets of 'incidents' and 'non-incidents'. As in the case of detecting misinformation, human observers should verify potential incidents for follow-up.

Concerns. Concerns similar to those in respect of observing misinformation on social media platforms arise here, including the possibility of missing information due to an overreliance on AI solutions and potential unequal performance. As such, tools should be used as supplements to existing methods of detecting incidents at polling places. Additionally, governments' mass collection of public data, especially concerning political subjects, raises serious concerns about surveillance, privacy and human rights, and could potentially pose a challenge to the freedom of expression (Inter-American Commission on Human Rights 2017).

Video monitoring

AI use case. AI-based video monitoring may serve several purposes during elections. AI models using closed-circuit television (CCTV) to monitor polling sites may be able to detect incidents or anomalies (e.g if a set of CCTV frames looks different from the average set of frames). Additionally, AI models may be useful for potentially detecting election fraud if a person appears twice at the same polling site or at multiple polling locations (Padmanabhan, Simoes and MacCarthaigh 2023). In all cases these incidents can be flagged for follow-up by EMB officials or election observers.

Implementation. Implementation will require extensive CCTV capabilities and the infrastructure to feed inputs from cameras into AI image and video recognition models. It may also be important to fine-tune models for tasks such as facial recognition and anomaly

Box 2.1. **Digital elections**

It is worth noting that AI may be useful for countries exploring new forms of voting and elections. For example, in countries with online voting systems where voters use their own devices, AI may be helpful for a variety of tasks. For example, online voting systems may use AI-based facial recognition software for identification, models trained on detecting bot activity or anomalous data on webpages for examining election fraud, and models meant to scan for cybersecurity threats to protect the integrity of servers. AI may also be useful in creating simulated user agents to test online voting systems for vulnerabilities and potential issues.

In countries exploring novel forms of democratic governance, such as online participatory democracy, LLMs may be useful for summarizing voters' positions and beliefs, and clustering models may be useful for grouping together similar ideas and statements (Eisen et al. 2023). For example, countries seeking to receive commentary on specific policies may build platforms where users can comment and share their opinions and then use a combination of AI and human oversight to better understand the beliefs of participants and, in some cases, even arrive at compromise solutions. In Taiwan, the vTaiwan program uses the Polis platform to solicit participatory feedback on policy positions, with AI models being used for summarization and clustering, and chatbots being used that speak on behalf of specific positions (Landemore 2023).

which could prompt a misallocation of EMB resources to investigate polling sites, potentially interfering in perfectly functional polling sites and missing actual issues at others. Developing secure and accurate systems for this use case is a technically challenging task, as models must account not only for the already difficult task of predicting total turnout rates but also for how turnout may vary throughout the electoral period.

2.4. **POST-ELECTORAL PERIOD**

The post-electoral period is the portion of the electoral cycle where the focus is largely on reviewing, analysing, reforming and strategizing an election.

2.4.1. **Electoral results analysis and reporting**

Post-electoral audits

AI use case. AI may be useful for post-election auditing practices. For example, AI may be used to detect incidents of fraud, and models developed prior to an election may provide comparisons with actual results. Additionally, machine learning and traditional statistics, such as difference-in-difference estimators, may be used to evaluate the efficiency and resource allocation of various polling sites. Clustering algorithms may be useful for spotting polling sites that demonstrate significant differences from other polling sites.

Implementation. Research has examined the role that both unsupervised and supervised algorithms trained on polling data may play in detecting election fraud. In some cases, these models use simulation techniques trained on polling and related election data to determine how similar actual results are to simulated ones. In general, these models require high levels of fraud in order to provide a high degree of accuracy, precision (i.e. a low number of false positives) and recall (i.e. a low number of false negatives) (Yamin et al. 2023). In lieu of polling, other attempts have used synthetic data, generating both a tampered and untampered version of election results, to train a model that is then applied to other elections. This work has found evidence that this technique may serve as a useful starting point for further election forensics research (Zhang, Alvarez and Levin 2019). Unsupervised algorithms may also be useful here, allowing EMBs to cluster polling sites and look for and flag potential anomalies (Green 2021). EMBs should consider the use of predefined probability thresholds to weed out false positives (e.g. only examining geographies where models predict a greater than 90 per cent chance of fraud having occurred).

Concerns. Since it is unlikely for EMBs to have access to data sets with perfectly labelled instances of election fraud, developing suitable supervised models for the task is difficult. A lack of ground truth data makes it difficult to evaluate the suitability of any model. Low recall and overreliance may result in EMBs missing instances of electoral fraud and other issues, whereas low precision may result in EMBs investigating high numbers of false positives. Both issues could undermine public faith in electoral integrity. EMBs considering

implementing this AI use case may mitigate some of these concerns by using it as only one piece of a broader auditing approach.

Political finance consolidation

AI use case. AI may be useful for the consolidation and auditing of political finance documents and reports during and after an election. OCR models may enable the scanning of physical receipts, and matching models may make it possible to develop auditing trails from political finance reports. LLMs and summarization models may also be useful in consolidating various campaign expenditures and donations into standardized formats for election officials to review. AI may be useful for detecting political finance fraud, such as cases where people donate under different names/addresses or make ineligible donations.

Implementation. Although we were unable to find research examining this specific use case, AI is increasingly being used in corporate financial auditing, which may offer some transferable practices. For example, the four largest global accounting firms (Deloitte, EY, KPMG and PwC) all offer some version of AI tools for corporate auditing, including anomaly detection, fraud detection, automated cash audits and pattern detection (Üçoğlu 2020). Modifications to similar tools may be useful for tracing political donations and expenditures. Computer vision and OCR tools can be used for data inputs, and GenAI tools may be useful for putting reporting documentation into standardized data formats to feed into auditing systems.

Concerns. AI tools used to consolidate data may suffer from hallucinations or other accuracy concerns, which could result in false positives or EMBs missing important information. Since there appear to be no tools created specifically for the task of political finance consolidation, work will also need to be done to fine-tune existing tools to meet the unique demands of EMBs, such as incorporating regulations on donation/spending limits, all of which may increase the complexity and decrease the effectiveness of AI approaches.

Cybersecurity risks

Any use of AI for elections is likely to introduce new cybersecurity concerns on top of additional AI-driven cyberthreats from other actors (see Chapter 3). For implementation, the cybersecurity risks are two-fold: first, the use of more digital technologies increases the attack surface (entry points) for cyber attackers, giving them more opportunities to find vulnerabilities within an electoral system. An increasing reliance on digital technologies as a part of the electoral process gives attackers novel ways to harm the integrity of elections. Second, the use of AI as a part of the electoral process also requires that EMBs collect more types of data, either about voters or about the election, such as voters' biometrics or camera feeds of polling sites. This increases both the pool of valuable data for attackers and the downsides if a successful cyberattack were to occur. The use of AI by malicious actors may increase the sophistication of cyberattacks. In practice, cybersecurity concerns can both directly and indirectly harm the integrity of elections. Directly, successful cyberattacks may prevent people from voting, change outcomes, disrupt voter registration databases and corrupt data. Indirectly, unsuccessful cyberattacks, or even just the threat of cyberattacks, could erode trust in the electoral system, dissuading certain subgroups of the population from participating in elections.

In many cases these are addressable concerns. To mitigate the cybersecurity risks associated with the use of AI, EMBs should consider conducting, in partnership with cybersecurity agencies and experts, cybersecurity audits of election systems to safeguard these new entry points. Adhering to the principle of data minimization may also decrease the overall cybersecurity risk, as EMBs should prioritize collecting as little private data as necessary to perform specific AI functions.

Overreliance on private companies

Due to the difficulty of the technical implementation of many of these use cases, EMBs' increasing reliance on private companies is another concern. At a minimum, AI usage requires technical infrastructure, such as GPUs (graphics processing units), that are produced and maintained by a small group of companies. In many cases EMBs are likely to require other computing infrastructure (e.g. cloud computing), technical talent from private companies and assistance

with cybersecurity practices. Meeting these requirements may give a select group of companies increasing power in the administration of elections, raising concerns about private sector influence within government and politics (Jungherr 2023).

Additionally, AI tools are likely to be developed by traditional vendors of election technologies. Procuring these technologies may slot easily into existing EMB practices, but it is worth noting that they may require significantly more testing and analysis by EMBs than normal.

To begin to mitigate some of these concerns, EMBs should work with other government agencies to consider whether AI use cases are feasible for internal development, and which ones may require private partnerships. EMBs should consider undertaking more thorough audits of privately developed technologies and set specific, high standards around efficacy and fairness for vendors. Setting standards for the transparency and accountability of privately developed technologies may also be important, especially when considering state policies on access to information about government decision-making processes.

Bias, discrimination, surveillance and human rights

There is a long history of AI and traditional statistical techniques being used to discriminate against specific groups of people, including through mass incarceration, denial of benefits and electoral discrimination (Crawford 2022). The ethics of AI are a well-studied subject, so in this Report we briefly cover areas for further examination by EMBs. Any use of AI systems that involves large amounts of data collection, especially by governments, risks perpetuating surveillance and its associated human rights violations. For example, AI that relies on the mass collection of public posts on social media may constitute surveillance that has the impact of dissuading free speech, even if these data are not misused (Inter-American Commission on Human Rights 2017). AI that relies on biometric data has similar concerns, potentially dissuading people from participating in electoral processes due to privacy or security concerns.

These risks multiply when understood through the lens of discrimination, with AI often being used to perpetuate existing

International Institute for Democracy and Electoral Assistance (International IDEA) examined the information environment in 53 countries, finding that the most common types of disinformation were attacks on the impartiality of EMBs, false or deceptive information about voting methods and conditions, and other attempts to deceive people into not voting (Bicu 2023). Offline and online disinformation techniques have long been used to mislead people—disproportionately marginalized communities—about election logistics and eligibility (Vandewalker 2020).

For this section, the primary question is the following: How does AI exacerbate this problem?

Using GenAI platforms and open-source models, malicious actors can quickly generate text, audio and video content with specific goals targeted at specific groups of people.

GenAI increases the quantity and improves the quality of the supply of traditional forms of disinformation, such as fake news articles and misleading posts on social media platforms. Using GenAI platforms and open-source models, malicious actors can quickly generate text, audio and video content with specific goals targeted at specific groups of people, often of a similar or higher quality than traditional human-written disinformation and with a lower likelihood of automated detection (Zhou et al. 2023). While the use of these platforms and models is unlikely to exacerbate issues with disinformation in areas where supply was not already a concern (e.g. posts targeted at large audiences on social media platforms), this improvement in capabilities may be an issue for previously neglected areas, such as small community social media groups, which attackers may have ignored in the past due to time and resource constraints. It is likely that the main threat of AI-based misinformation is at the community level, where EMBs are less likely to become aware of its spread and where disinformation by malicious actors can be hyper-targeted at specific groups or individuals. Misinformation may be spread on a variety of platforms, including major social media networks, email lists, search engines and private messaging services. For the latter, detecting misinformation will be difficult, as encrypted messaging platforms are unable to moderate the content shared in messages.

GenAI offers new capabilities for disinformation, including the generation of high-quality audio and video deepfakes. The risks of these forms of disinformation may be country-specific. In Canada

and the USA, for example, we believe that a major threat of AI disinformation is the development of audio deepfakes to imitate political candidates, election officials and local community leaders, and to use those imitations to call voters and deceive them about election processes (Bond 2024). There is already evidence of this occurring in US elections (Hsu 2024). This threat is most pronounced when executed in small, targeted communities, where officials are less likely to learn of disinformation until it has spread.

Video deepfakes are likely to be used for similar purposes and may be an important threat in other countries. Although video deepfakes are still unable to perfectly imitate the realism of actual video, these remain a serious concern among communities with lower levels of digital literacy. Just before Pakistan's most recent general elections, multiple deepfake videos were spread on platforms across the country, including fake videos of politicians declaring boycotts of the vote, potentially impacting electoral integrity (Mughal 2024). Although we do not currently have evidence of the efficacy of video or audio deepfakes on electoral integrity in a global context, EMBs should be prepared for an increase in the quantity and an improvement in the quality of this type of disinformation.

There is the additional concern of higher-quality misinformation further obscuring trust in any online information. This may incentivize candidates and other relevant parties to use the 'liar's dividend' and claim that legitimate recordings or pictures are AI-generated. This is likely to result in a general decrease in trust in information, making the job of spreading accurate information for EMBs more difficult. Additionally, there is evidence that excessively worrying people about the spread of disinformation is unlikely to decrease their susceptibility to it while potentially increasing their willingness to support restrictions on the freedom of expression (Jungherr and Rauchfleisch 2024).

It is worth noting that, due to the general public's adoption of AI chatbots, it is conceivable that voters could ask chatbots such as ChatGPT and Gemini questions about elections, such as when they will take place, where one can vote, and if they are safe and secure. As in the case of voters using search engines for this purpose, this use of chatbots raises concerns about information accuracy. Since

not all LLM chatbots have Internet access, and they are often trained on outdated information, coupled with their tendency to hallucinate, it is conceivable that these chatbots could provide incorrect information about voter eligibility and the logistics of elections. In some cases GenAI platforms have announced plans to partner with authoritative sources of election information that they can direct users with questions to, but the effectiveness and scope of these plans, especially outside the USA, are still unknown (OpenAI 2024).

Political campaigns in various countries have been using data science and machine learning techniques as a part of their strategies for some time.

3.2. **POLITICAL ORGANIZATIONS**

Political campaigns in various countries have been using data science and machine learning techniques as a part of their strategies for some time, with several prominent recent examples being Barack Obama's 2012 US presidential campaign's use of data science for organizing and fundraising, the 2016 Cambridge Analytica scandal in the United Kingdom and the USA, and increasing usage in Indian elections (Dommett 2019; Varna 2019).

Political organizations are likely to use AI for various tasks, some of which may be important to EMBs. There is evidence that highly personalized microtargeting for political advertising may be more effective than generic advertising on social media platforms (Simchon, Edwards and Lewandowsky 2024). Campaigns and other political organizations may use AI to develop specific advertising targeting individuals or small groups of the population to influence their voting behaviour. In countries where EMBs are responsible for monitoring campaign communications, this may drastically increase the workload for EMBs, with campaigns using AI to generate more versions of the same advertisement. EMBs may have to rethink their processes around campaign advertising reporting and monitoring. Given the possibility of GenAI models hallucinating or producing false information, the risks of these advertisements may increase, especially when organizations use fully automated systems. Political organizations may knowingly use GenAI to develop and spread disinformation. Addressing these issues may require more EMB regulation and oversight and, in some cases, partnerships with other government agencies or changes in EMB mandates.

Other forms of public-facing AI strategies on the part of campaigns may also be relevant for EMBs. Political candidates around the world have already used GenAI to create deepfakes of themselves giving speeches or speaking in foreign languages (Calma 2023; Zhuang 2024). For EMBs responsible for monitoring campaign communications, this kind of AI usage may raise complex questions around definitions of misinformation or misleading communication. Campaigns in various countries, including Indonesia and Pakistan, have begun to create fine-tuned chatbots that mimic candidates or provide information for voters to interact with (Parkin and Bokhari 2024; Rayda 2024). These chatbots present similar problems to those posed by general chatbots, in that the responses to users' election-related questions may suffer from inaccuracies.

Political organizations are likely to use AI for a variety of other campaign tasks, such as speech/content writing, resource allocation, strategy organization, internal analytics and crowdsourcing of policy positions. On some occasions these AI use cases may impact the work of EMBs. For example, campaigns may use AI to build better data analytics capabilities, helping them decide where to focus their efforts when advertising, knocking on doors or hosting events. For EMBs with mandates to protect the data privacy rights of voters, the use of AI, which generally requires larger data sets compared with traditional statistical methods, may raise concerns. Additionally, if these methods are successful, this may impact turnout rates, requiring EMBs to reconsider resource allocation at polling sites or in different geographies.

3.3. SECURITY THREATS TO ELECTION SYSTEMS

Electoral systems and EMBs have long been targets of cyberattacks.

Electoral systems and EMBs have long been targets of cyberattacks (Van der Staak and Wolf 2019). Although there are many cybersecurity threats to EMBs and other agencies responsible for elections, in this Report we focus exclusively on the area where advances in AI may exacerbate the problem in the short term—namely, through higher-quality phishing attempts. Although advances in AI are likely to improve the quality of malware and exploit development techniques, the primary near-term risk of AI for

EMB-related cybersecurity is an advance in the quality of phishing (National Cyber Security Centre 2024).

Hackers targeting elections often use social engineering (i.e. tactics to manipulate, influence or deceive victims) to gain access to private systems, commonly through phishing attacks. Phishing involves deceiving recipients into believing that communications are from trusted sources and leveraging that deception to have victims communicate sensitive information or download harmful files. In the past, widescale phishing attempts have generally been low-quality, given the time commitment required to create high-quality fraudulent communications when targeting specific individuals (commonly known as spear phishing). Much like in the case of disinformation, generative AI makes the process of finding potential victims and generating high-quality content substantially more efficient, potentially increasing the odds of success (Norden and Ramachandran 2023). Fine-tuning language models by using previous official communications or feeding them information about the structure of election offices could result in the generation of highly convincing and legitimate-seeming outputs (Gupta et al. 2023).

AI is likely to exacerbate text-based phishing, which is the most common, as well as bolster newer forms of phishing, such as voice-mimics and phone calls of senior officials (Cybersecurity and Infrastructure Security Agency 2024). Successful phishing attempts may result in election officials divulging confidential data or giving attackers access to key systems, such as EMB websites, voter data sets, registration databases or even election results.

Additionally, EMBs that provide platforms where constituents can submit complaints or requests for information to officials may be vulnerable to AI-based information flooding. For example, EMBs that operate a system for voters to submit issues at polling places may receive realistic, but false, AI-generated statements. A flood of such issues could overwhelm technical systems designed to deal with small numbers of complaints, crowd out actual issues at polling places or result in EMBs making decisions based on false information.

3.4. **PATHS FORWARD**

Below, we offer a series of recommendations for EMBs and other relevant parties to address some of the concerns discussed in this section. It is worth noting that, in almost all cases, advances in AI are simply exacerbating existing areas of concern for EMBs, and the best mitigation methods involve enhancing existing security practices.

1. EMBs should work closely with local officials and community interest groups to identify the spread of misinformation around elections. EMBs should set up methods for reporting election misinformation to the EMB and other government agencies.

2. EMBs should have a verified presence on major platforms to combat the spread of misinformation and should be quick to respond to instances of misinformation. EMBs should amplify accurate and informative content around elections.

3. If it is within their mandate to do so, EMBs should proactively engage with major social media and GenAI platforms to make the necessary resources available to pre-bunk and debunk electoral misinformation. They should also work to make electoral information available in machine-readable formats such that platforms can easily integrate correct and accurate information into user-facing content.

4. EMBs should cooperate with other government agencies, such as communications regulators and cybersecurity agencies, to prevent the proliferation of disinformation and to hold the responsible parties accountable, including by preventing call/number spoofing, as well as regulating robocalls and the use of AI deepfakes on communication networks.

5. EMBs should strengthen existing cybersecurity practices through the use of anti-phishing tools, staff training, multifactor authentication, and other forms of collaboration with cybersecurity agencies and experts. EMBs should mandate similar measures for election technology vendors.

6. EMBs should work with, and hold accountable, GenAI platforms to prevent the use of their tools for spreading election-related misinformation. Steps could include everything from regulating the use and development of GenAI tools to providing platforms with accurate information regarding election logistics. EMBs should require GenAI platforms to have transparent guidelines about how their tools can be used for political events, and how those rules will be enforced.

7. EMBs should hold social media platforms accountable and ensure that appropriate moderation decisions are being made in accordance with domestic and international norms and laws.

8. EMBs should inform political organizations of potential information-related threats and hold parties accountable for their use of AI. Possible actions include mandating that AI usage for political purposes is made transparent and that political organizations are barred from spreading disinformation about election-related logistics.

9. EMBs should specifically consider the impact of AI across all of these mitigation strategies with a focus on marginalized communities, who are especially targeted in disinformation campaigns and most vulnerable to the perpetuation of biases by AI models.

Chapter 4

AI REGULATORY FRAMEWORKS AND IMPLICATIONS FOR ELECTIONS

The legal landscape around AI use is still developing, with a variety of approaches being considered and implemented in different countries. In this chapter we offer a brief discussion of some AI regulatory frameworks and how they could impact the work of electoral authorities.

The legal landscape around AI use is still developing, with a variety of approaches being considered and implemented in different countries.

4.1. **EU AI ACT**

The EU AI Act[2] focuses on regulating the development and use of AI systems in EU member states. The AI Act was endorsed by the European Parliament in March 2024, with its application starting gradually from 2024 onwards (Chee 2024).

Most research on the AI Act focuses on the implications of the regulation for private companies, but the use of AI by EU governments is also covered by its rules. In this section we focus on the potential regulatory implications of the AI Act on the implementation of AI systems by EMBs and other electoral authorities.

The AI Act takes a risks-based approach to the regulation of AI systems, categorizing use cases based on four levels of risk—unacceptable, high, limited and minimal.

2 As of the time of writing, the AI Act is not yet in force. This Report should be taken as a preliminary view of the Act's potential implications for the use of AI within EMBs in EU member states.

Many use cases of AI for electoral management are likely to fall into the high-risk category.

Many use cases of AI for electoral management are likely to fall into the high-risk category, which covers systems used for the 'administration of justice and democratic processes', including 'AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view' (European Parliament and Council of the European Union 2024: 40, 40a).

It is worth noting that the AI Act prohibits (with some exceptions, including for national security purposes) the use of AI systems with unacceptable risk. Relevant for EMBs using and regulating AI, this prohibition includes the following:

- deploying subliminal, manipulative or deceptive techniques to distort behaviour and impair informed decision making, causing significant harm;
- compiling facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage; and
- real-time remote biometric identification in publicly accessible spaces for law enforcement (with some exceptions).

The AI Act mostly regulates the providers of high-risk systems, which may be either election technology vendors or EMBs themselves. It also regulates so-called deployers, which would include EMBs using both internally and externally developed AI. For high-risk systems, some requirements for providers include establishing risk management systems, conducting data governance, allowing for human oversight, and achieving appropriate levels of accuracy, robustness and cybersecurity; for deployers of high-risk systems, some requirements include assigning human oversight to qualified people, monitoring and operating the system according to the usage instructions and informing providers about issues (European Parliament and Council of the European Union 2024).

The AI Act's risk-based framework offers a helpful way for EMBs to navigate the prospect of implementing AI for electoral processes. Examining how serious the risks of an AI use case may be (e.g. impacting electoral outcomes or simply making an existing process more efficient) and taking the proposed steps for that level of risk, including analysing the necessity and proportionality of the use case, may be a good starting point. For high-risk systems, the AI Act's requirements of ensuring human oversight, carrying out model performance audits and conducting data governance are key ways to mitigate some of the concerns associated with AI implementation.

4.2. **US ARTIFICIAL INTELLIGENCE EXECUTIVE ORDER**

Another potentially relevant piece of regulation is the US Government's Artificial Intelligence Executive Order (AI Executive Order) (United States of America 2023). The AI Executive Order covers the use of AI by US Government authorities, and as a result it could impact the use of AI for electoral management within the USA. In particular the AI Executive Order includes provisions to:

- direct federal agencies to develop and use tools to verify the authenticity of government communications;
- evaluate and strengthen how federal agencies procure and use commercial data sets, and strengthen privacy guidance;
- issue guidance for federal agencies' use of AI, including on how to protect rights and safety; and
- address civil rights and civil liberties violations relating to AI usage in the private and public sector.

It is worth noting that the AI Executive Order is not US legislation; rather, it is an executive directive focused mostly on allocating federal resources and clarifying the enforcement of existing laws in the context of AI. The USA, like many other countries, is in discussions regarding comprehensive AI legislation akin to the AI Act that could further impact the work of electoral authorities.

4.3. **BRAZILIAN ELECTORAL COURT REGULATIONS**

Potentially relevant are the recent electoral regulations adopted by Brazil's Superior Electoral Court (Conceição 2024). This is a rare example of AI regulation specifically tailored to elections. Much of the regulation covers the use of AI for political campaigning, requiring that:

- campaigns clearly watermark all AI-generated electoral campaign content;
- fabricated or manipulated content for misinformation purposes is completely prohibited;
- misinformation that could harm electoral integrity is completely prohibited; and
- campaigns do not create deepfakes or chatbots to emulate interactions between candidates and the public.

The regulations require that platforms that host or broadcast electoral content adopt measures to prevent the spread of any of these violations.

4.4. **AI REGULATION IN OTHER COUNTRIES**

Several other countries, including Argentina, Canada, Chile, Colombia, India, Japan, New Zealand, Peru, Singapore and many more, either have passed AI-related guidance or are in the process of developing AI-related regulations (IAPP 2024). Many of these regulations take risk-based approaches, focusing on the highest-risk AI use cases in both the public and private sectors. It is likely that, in many countries, many EMB-related AI use cases, as well as many third-party use cases that will affect EMBs, will fall into higher-risk categories given their potential impact on democracy.

Chapter 5

CONCLUSION

This Report provides a broad overview of the AI-related opportunities and challenges for elections. It illustrates EMBs' potential to use AI to improve electoral processes across the entire electoral cycle, including for voter registration, election planning, civic education, campaign and media monitoring, voting operations, polling place monitoring, vote tabulation and results analysis. EMBs considering rapid implementation of AI may also look to the use of generalist GenAI tools for employees, such as using Microsoft's Copilot, for help with drafting or summarizing emails and content.

Although many of these use cases are promising, they all raise concerns. In practice, the technical difficulty in implementing, monitoring and maintaining some AI systems, as well as the unreliability of many models, poses serious questions regarding the ability of EMBs to deploy and manage AI while also maintaining electoral integrity. Reliability concerns have possible ethical implications, with AI use potentially raising issues of bias and discrimination, especially for historically marginalized communities. AI use may decrease public trust in elections, especially when it requires increased surveillance, potentially causing a chilling effect for human rights.

Although many of these use cases are promising, they all raise concerns.

EMBs considering the use of AI should focus on the principles of necessity, data minimization and proportionality, paying specific attention to the costs and benefits of using AI in place of existing practices. Implementing strong standards of transparency, cybersecurity, testing, auditing and human oversight may help mitigate some of the concerns with AI usage, but EMBs considering

implementation should start by focusing on use cases with the lowest potential risks. In almost all cases, EMBs should first focus on building the infrastructure, technical expertise and ethics/auditing practices required to safely use AI before procuring or developing it.

For the use of AI by non-EMB actors, it is critical that EMBs develop plans to respond to the ways AI could impact electoral management. For example, it is likely that EMBs will see an uptick in both the quantity and quality of election-related misinformation. Although AI may not drastically alter the misinformation landscape, it could further complicate trust in electoral processes, and EMBs should take steps to combat misinformation, especially disinformation targeting marginalized communities, including by working with local officials, community groups, GenAI companies and social media platforms.

Political campaigns and organizations are likely to use AI to influence elections for generating content/advertising, data analytics and other campaign tasks. For EMBs whose mandates include the monitoring of political organizations, EMBs should work with other government agencies to limit disinformation from campaigns, require watermarking of AI-generated content and consider the privacy implications of campaigns' AI use.

EMBs should be aware of the increased cybersecurity threat posed by AI, both when implementing AI and in its use by external actors. In particular, EMBs should be prepared for higher-quality phishing attempts that use GenAI to manipulate people into sharing internal information. Working closely with cybersecurity experts, following existing recommended cybersecurity practices and training employees on this threat are all steps worth considering.

EMBs should work closely with their governments to understand the implications of various regulatory frameworks and how they may impact the work of EMBs. For example, EMBs considering AI implementation within the EU may have their use cases fall into the 'high-risk' category, requiring them to meet higher standards of transparency, accountability and human oversight than for other technologies. EMBs may have to amend their own mandates and regulatory structures in order to preserve their ability to ensure electoral integrity.

Finally, as AI and the regulation of AI are rapidly evolving fields, EMBs should consider this Report as a broad, non-comprehensive overview of the role AI could play in their elections. EMBs should keep abreast of AI development, opportunities and risks, and collaborate closely with experts within and outside of government to continuously update their understanding of the landscape. With this Report we hope to offer a starting point for those discussions.

References

Akbar, P., Jafar Loilatu, M., Pribadi, U. and Sudiar, S., 'Implementation of artificial intelligence by the General Elections Commission in creating a credible voter list', *IOP Conference Series: Earth and Environment Science*, 717/1 (2021), <https://doi.org/10.1088/1755-1315/717/1/012017>

Al-Haidary, M., Ajlouni, M. A., Talib, M. A., Abbas, S., Nasir, Q. and Basaeed, E., 'Metaheuristic approaches to facility location problems: A systematic review', in *4th International Conference on Signal Processing and Information Security* (Institute of Electrical and Electronics Engineers, 2021), pp. 49–52, <https://doi.org/10.1109/ICSPIS53734.2021.9652430>

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. and Rieke, A., 'Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes', ArXiv, 12 September 2019, <https://doi.org/10.48550/arXiv.1904.02095>

Barretto, S., Chown, W., Meyer, D., Soni, A., Tata, A. and Halderman, J. A., 'Improving the accuracy of ballot scanners using supervised learning', in R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak and M. Germann (eds), *Electronic Voting: 6th International Joint Conference, E-Vote-ID 2021, Virtual Event, October 5–8, 2021, Proceedings* (Springer International Publishing, 2021), pp. 17–32, <https://doi.org/10.1007/978-3-030-86942-7_2>

Bender, S. M. L., 'Algorithmic elections', *Michigan Law Review*, 121/3 (2022), pp. 489–524, <https://doi.org/10.36644/mlr.121.3.algorithmic>

Bicu, I., 'The information environment around elections', International IDEA, 2023, <https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections>, accessed 15 April 2024

Bond, S., 'AI fakes raise election risks as lawmakers and tech companies scramble to catch up', NPR, 8 February 2024, <https://www.npr.org/2024/02/08/1229641751/ai-deepfakes-election-risks-lawmakers-tech-companies-artificial-intelligence>, accessed 15 April 2024

Brynjolfsson, E., Li, D. and Raymond, L. R., 'Generative AI at Work', National Bureau of Economic Research, Working Paper 31161, November 2023, <https://doi.org/10.3386/w31161>

Calma, J., 'NYC Mayor Eric Adams uses AI to make robocalls in languages he doesn't speak', *The Verge*, 17 October 2023, <https://www.theverge.com/2023/10/17/23920733/nyc-mayor-eric-adams-ai-robocalls-spanish-mandarin>, accessed 15 April 2024

Carrasco, M., Habib, C., Felden, F., Sargeant, R., Mills, S., Shenton, S., Ingram, J. and Dando, G., 'Generative AI for the public sector: The journey to scale', Boston Consulting Group, 26 March 2024, <https://www.bcg.com/publications/2024/gen-ai-journey-to-scale-in-government>, accessed 15 April 2024

Chee, F. Y., 'Europe one step away from landmark AI rules after lawmakers' vote', Reuters, 14 March 2024, <https://www.reuters.com/technology/eu-lawmakers-endorse-political-deal-artificial-intelligence-rules-2024-03-13>, accessed 15 April 2024

Clark, A., 'The cost of democracy: The determinants of spending on the public administration of elections', *International Political Science Review*, 40/3 (2019), pp. 354–69, <https://doi.org/10.1177/0192512118824787>

Conceição, L. H. M., 'Brazilian judges regulate elections … and AI', Verfassungsblog, 15 March 2024, <https://doi.org/10.59704/612f31a89ce38fc6>

Crawford, K., *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* (New Haven, CT: Yale University Press, 2022), <https://doi.org/10.12987/9780300252392>

Cybersecurity and Infrastructure Security Agency, 'Risk in focus: Generative A.I. and the 2024 election cycle', 18 January 2024, <https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_ElectionsV2_508c.pdf>, accessed 15 April 2024

Dhiman, P., Kaur, A., Iwendi, C. and Mohan, S. K., 'A scientometric analysis of deep learning approaches for detecting fake news', *Electronics*, 12/4 (2023), p. 948, <https://doi.org/10.3390/electronics12040948>

Dommett, K., 'Data-driven political campaigns in practice: Understanding and regulating diverse data-driven campaigns', *Internet Policy Review*, 8/4 (2019), <https://doi.org/10.14763/2019.4.1432>

Eisen, N., Lee, N. T., Galliher, C. and Katz, J., 'AI can strengthen U.S. democracy—and weaken it', Brookings, 21 November 2023, <https://www.brookings.edu/articles/ai-can-strengthen-u-s-democracy-and-weaken-it>, accessed 15 April 2024

Electronic Registration Information Center, Technology and Security Brief 6.1, 8 March 2024, <https://ericstates.org/wp-content/uploads/documents/ERIC-Tech-Security-Brief.pdf>, accessed 15 April 2024

European Parliament and Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', 2021/0106 (COD), 2024, <https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf>, accessed 15 April 2024

Goel, S., Meredith, M., Morse, M., Rothschild, D. and Shirani-Mehr, H., 'One person, one vote: Estimating the prevalence of double voting in U.S. presidential elections', *American Political Science Review*, 114/2 (2020), pp. 456–69, <https://doi.org/10.1017/S000305541900087X>

Green, J., 'Anomaly detection in election data and its representation of U.S. infrastructure vulnerability', in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference* (Institute of Electrical and Electronics Engineers, 2021), pp. 503–08, <https://doi.org/10.1109/IEMCON53756.2021.9623111>

Gstrein, O. J., Bunnik, A. and Zwitter, A., 'Ethical, legal and social challenges of predictive policing', *Católica Law Review, Direito Penal*, 3/3 (2019), pp. 77–98, <https://papers.ssrn.com/abstract=3447158>, accessed 15 April 2024

Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L., 'From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy', *IEEE Access*, 11 (2023), pp. 80218–45, <https://doi.org/10.1109/ACCESS.2023.3300381>

Haenschen, K., 'The conditional effects of microtargeted Facebook advertisements on voter turnout', *Political Behavior*, 45/1 (2022), pp. 1661–81, <https://doi.org/10.1007/s11109-022-09781-7>

Hajnal, Z., Kuk, J. and Lajevardi, N., 'We all agree: Strict voter ID laws disproportionately burden minorities', *The Journal of Politics*, 80/3 (2018), pp. 1052–59, <https://doi.org/10.1086/696617>

Hardyns, W. and Rummens, A., 'Predictive policing as a new tool for law enforcement? Recent developments and challenges', *European Journal on Criminal Policy and Research*, 24/3 (2018), pp. 201–18, <https://doi.org/10.1007/s10610-017-9361-2>

Hsu, T., 'New Hampshire officials to investigate A.I. robocalls mimicking Biden', *The New York Times*, 22 January 2024, <https://www.nytimes.com/2024/01/22/business/media/biden-robocall-ai-new-hampshire.html>, accessed 15 April 2024

Hsu, T., Thompson, S. A. and Myers, S. L., 'Elections and disinformation are colliding like never before in 2024', *The New York Times*, 9 January 2024, <https://www.nytimes.com/2024/01/09/business/media/election-disinformation-2024.html>, accessed 15 April 2024

Hussain, R., Raza, A., Siddiqi, I., Khurshid, K. and Djeddi, C., 'A comprehensive survey of handwritten document benchmarks: Structure, usage and evaluation', *EURASIP Journal on Image and Video Processing*, 1 (2015), <https://doi.org/10.1186/s13640-015-0102-5>

Inter-American Commission on Human Rights, 'Standards for a Free, Open and Inclusive Internet', OEA/Ser.L/V/II. OAS, 15 March 2017, <https://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf>, accessed 15 April 2024

International Association of Privacy Professionals (IAPP), 'Global AI Law and Policy Tracker', February 2024, <https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf>, accessed 15 April 2024

Juneja, P. and Floridi, L., 'Using Twitter to detect polling place issues on U.S. election days', SSRN, 24 January 2023, <https://doi.org/10.2139/ssrn.4334243>

Jungherr, A., 'Artificial intelligence and democracy: A conceptual framework', *Social Media + Society*, 9/3 (2023), <https://doi.org/10.1177/20563051231186353>

Jungherr, A. and Rauchfleisch, A., 'Negative downstream effects of alarmist disinformation discourse: Evidence from the United States', *Political Behavior* (2024), <https://doi.org/10.1007/s11109-024-09911-3>

Kan, H. J., Kharrazi, H., Chang, H.-Y., Bodycombe, D., Lemke, K. and Weiner, J. P., 'Exploring the use of machine learning for risk adjustment: A comparison of standard and penalized linear regression models in predicting health care costs in older adults', *PloS One*, 14/3 (2019), <https://doi.org/10.1371/journal.pone.0213258>

Kennedy, R., Wojcik, S. and Lazer, D., 'Improving election prediction internationally', *Science*, 355/6324 (2017), pp. 515–20, <https://www.science.org/doi/10.1126/science.aal2887>

Kondamudi, M. R., Sahoo, S. R., Chouhan, L. and Yadav, N., 'A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches', *Journal of King*

Saud University - Computer and Information Sciences, 35/6 (2023), <https://doi.org/10.1016/j.jksuci.2023.101571>

Kwon, C., Moreno, A. and Raman, A., 'The impact of input inaccuracy on leveraging AI tools: Evidence from algorithmic labor scheduling', SSRN, 22 October 2023, <https://doi.org/10.2139/ssrn.4602747>

Landemore, H., 'Fostering more inclusive democracy with AI', International Monetary Fund, December 2023, <https://www.imf.org/en/Publications/fandd/issues/2023/12/POV-Fostering-more-inclusive-democracy-with-AI-Landemore>, accessed 15 April 2024

Liu, Z. and Hu, S., 'Predicting the fundraising performance of environmental crowdfunding projects: An interpretable machine learning approach', *Information Processing & Management*, 61/2 (2024), <https://doi.org/10.1016/j.ipm.2023.103587>

Livemint, 'EC to start campaign to link voter ID with Aadhaar from August 1. Check details here', *Mint*, 25 July 2022, <https://www.livemint.com/news/india/ec-to-start-campaign-to-link-voter-id-with-aadhaar-from-august-1-check-details-here-11658748573098.html>, accessed 15 April 2024

Mann, C. and Stein, R. M., 'The Impact of Polling Places on Voting', Paper prepared for the Election Science Reform and Administration Conference, University of Pennsylvania, Philadelphia, PA, July 2019, <https://web.sas.upenn.edu/esra2019/files/2019/07/Mann-and-Stein-Polling-Place-Effect.pdf>, accessed 15 April 2024

Markay, L., 'AI becomes a political "super-weapon"', *Axios*, 7 October 2022, <https://www.axios.com/2022/10/07/ai-becomes-a-political-super-weapon>, accessed 15 April 2024

MIT Election Data Science Lab, 'Voting technology', 21 April 2023, <https://electionlab.mit.edu/research/voting-technology>, accessed 15 April 2024

Mökander, J. and Floridi, L., 'Ethics-based auditing to develop trustworthy AI', *Minds and Machines*, 31/2 (2021), pp 323–27, <https://doi.org/10.1007/s11023-021-09557-8>

Moses, L. and Box-Steffensmeier, J. M., 'Considerations for Machine Learning Use in Political Research with Application to Voter Turnout', 2021, <https://polmeth.theopenscholar.com/files/polmeth/files/moses-box-steffensmeier-2020.pdf>, accessed 15 April 2024

Mughal, N., 'Deepfakes, Internet access cuts make election coverage hard, journalists say', Voice of America, 22 February 2024, <https://www.voanews.com/a/deepfakes-internet-access-cuts-make-election-coverage-hard-journalists-say-/7498917.html>, accessed 15 April 2024

Muppasani, B., Pallagani, V., Lakkaraju, K., Lei, S., Srivastava, B., Robertson, B., Hickerson, A. and Narayanan, V., 'On safe and usable chatbots for promoting voter participation', *AI Magazine*, 44/3 (2023), pp. 240–47, <https://doi.org/10.1002/aaai.12109>

National Cyber Security Centre, 'The Near-Term Impact of AI on the Cyber Threat', 24 January 2024, <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>, accessed 15 April 2024

Norden, L. and Ramachandran, G., 'Artificial intelligence and election security', Brennan Center for Justice, 5 October 2023, <https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-and-election-security>, accessed 15 April 2024

Noy, S. and Zhang, W., 'Experimental evidence on the productivity effects of generative artificial intelligence', *Science*, 381/6654 (2023), pp. 187–92, <https://www.science.org/doi/10.1126/science.adh2586>

OpenAI, 'How OpenAI is approaching 2024 worldwide elections' [blog], 15 January 2024, <https://openai.com/blog/how-openai-is-approaching-2024-worldwide-elections>, accessed 15 April 2024

Organisation for Economic Co-operation and Development, 'Recommendation of the Council on Artificial Intelligence', OECD/LEGAL/0449, adopted 22 May 2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>, accessed 15 April 2024

Padmanabhan, D., Simoes, S. and MacCarthaigh, M., 'AI and core electoral processes: Mapping the horizons', *AI Magazine*, 44/3 (2023), pp. 218–39, <https://doi.org/10.1002/aaai.12105>

Parkin, B. and Bokhari, F., 'Imran Khan taps AI and TikTok to fight Pakistan election from jail', *Financial Times*, 1 February 2024, <https://www.ft.com/content/7c3c5827-c965-453c-8bd1-d1312e90669a>, accessed 15 April 2024

Pech, L., 'The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU', Open Society European Policy Institute, March 2021, <https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf>, accessed 15 April 2024

Perkowitz, S., 'The bias in the machine: Facial recognition technology and racial disparities', *MIT Case Studies in Social and Ethical Responsibilities of Computing*, Winter (2021), <https://doi.org/10.21428/2c646de5.62272586>

Rawte, V., Sheth, A. and Das, A., 'A survey of hallucination in large foundation models', ArXiv, 12 September 2023, <https://doi.org/10.48550/arXiv.2309.05922>

Rayda, N., 'Indonesia elections 2024: How AI has become a double-edged sword for candidates and election officials', CNA, 4 February 2024, <https://www.channelnewsasia.com/asia/ai-disinformation-deepfakes-indonesia-elections-4091296>, accessed 15 April 2024

Richardson, R., Schultz, J. and Crawford, K., 'Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice', *New York University Law Review Online*, 94/192 (2019), <https://papers.ssrn.com/abstract=3333423>, accessed 15 April 2024

Simchon, A., Edwards, M. and Lewandowsky, S., 'The persuasive effects of political microtargeting in the age of generative artificial intelligence', *PNAS Nexus*, 3/2 (2024), p. 35, <https://doi.org/10.1093/pnasnexus/pgae035>

Solender, A. and Fried, I., 'Scoop: Congress bans staff use of Microsoft's AI Copilot', *Axios*, 29 March 2024, <https://www.axios.com/2024/03/29/congress-house-strict-ban-microsoft-copilot-staffers>, accessed 15 April 2024

Stokel-Walker, C., 'AI chatbot models "think" in English even when using other languages', *New Scientist*, 8 March 2024, <https://www.newscientist.com/article/2420973-ai-chatbot-models-think-in-english-even-when-using-other-languages>, accessed 15 April 2024

Suhenda, D., 'KPU insists on using Sirekap', *The Jakarta Post*, 22 February 2024, <https://www.thejakartapost.com/indonesia/2024/02/22/kpu-insists-on-using-sirekap.html>, accessed 15 April 2024

Talarico, L. and Maya Duque, P. A., 'An optimization algorithm for the workforce management in a retail chain', *Computers & Industrial Engineering*, 82 (2015), pp. 65–77, <https://doi.org/10.1016/j.cie.2015.01.014>

Üçoğlu, D., 'Current machine learning applications in accounting and auditing', *Pressacademia*, 12/1 (2020), pp. 1–7, <https://doi.org/10.17261/Pressacademia.2020.1337>

UN Refugee Agency (UNHCR), Factsheet 4: Types of Misinformation and Disinformation, February 2022, <https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf>, accessed 22 April 2024

United States of America, 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence', The White House, 20 October 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>, accessed 15 April 2024

Valle-Cruz, D., Fernandez-Cortez, V. and Gil-Garcia, J. R., 'From e-budgeting to smart budgeting: Exploring the potential of artificial intelligence in government decision-making for resource allocation', *Government Information Quarterly*, 39/2 (2022), <https://doi.org/10.1016/j.giq.2021.101644>

Van Brakel, R., 'Pre-emptive big data surveillance and its (dis)empowering consequences: The case of predictive policing', in B. van der Sloot, D. Broeders and E. Schrijvers (eds), *Exploring the Boundaries of Big Data* (The Hague, Amsterdam: Amsterdam University Press, 2016), pp. 117–41, <https://doi.org/10.2139/ssrn.2772469>

Van der Staak, S. and Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration* (Stockholm: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>

Vandewalker, I., 'Digital Disinformation and Vote Suppression', Brennan Center for Justice, 2 September 2020, <https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression>, accessed 15 April 2024

Varna, A., 'Big data analytics and transformation of election campaign in India', SSRN, 30 December 2019, <https://doi.org/10.2139/ssrn.3511428>

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L. and Polosukhin, I., 'Attention is all you need', ArXiv, 6 December 2017, <http://arxiv.org/abs/1706.03762>, accessed 15 April 2024

Wei, A., Haghtalab, N. and Steinhardt, J., 'Jailbroken: How does LLM safety training fail?', ArXiv, 5 July 2023, <https://doi.org/10.48550/arXiv.2307.02483>

Wolf, P., Alim, A., Kasaro, B., Namugera, P., Saneem, M. and Zorigt, T., *Introducing Biometric Technology in Elections* (Stockholm: International IDEA, 2017), <https://www.idea.int/publications/catalogue/introducing-biometric-technology-elections>, accessed 15 April 2024

Yamin, K., Jadali, N., Xie, Y. and Nazzal, D., 'Novelty detection for election fraud: A case study with agent-based simulation data', *AI Magazine*, 44/3 (2023), pp. 255–62, <https://doi.org/10.1002/aaai.12112>

Zhang, M., Alvarez, R. M. and Levin, I., 'Election forensics: Using machine learning and synthetic data for possible election anomaly detection', *PloS One*, 14/10 (2019), <https://doi.org/10.1371/journal.pone.0223950>

Zhao, F., Zhang, C., Saxena, N., Wallach, D. and Rabby, A. S. A., 'Ballot tabulation using deep learning', in *2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science* (Institute of Electrical and Electronics Engineers, 2023), pp. 107–14, <https://doi.org/10.1109/IRI58017.2023.00026>

Zhou, J., Zhang, Y., Luo, Q., Parker, A. G. and De Choudhury, M., 'Synthetic lies: Understanding AI-generated misinformation and evaluating algorithmic and human solutions', in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (New York, NY: Association for Computing Machinery, 2023), pp. 1–20, <https://doi.org/10.1145/3544548.3581318>

Zhuang, Y., 'Imran Khan's "victory speech" from jail shows A.I.'s peril and promise', *The New York Times*, 11 February 2024, <https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html>, accessed 15 April 2024

Annex A. Key terms

Below, we offer some explanations of technical and non-technical AI-related terms for the purposes of this Report. These are not meant to be comprehensive definitions, but rather to help this Report's audience understand the text.

Term	Explanation
Accuracy	A measurement of what percentage of inputs a model classifies correctly.
Deep learning	Used to reference a subset of machine learning that uses multilayered neural networks, generally of large size, with large data sets, to accomplish prediction tasks. Most mainstream examples of recent advances in machine learning, such as large language models, fit into this category.
Discriminative AI	Refers to a subset of machine learning where models are used to classify or separate data. LLMs used to classify text as 'positive' or 'negative' sentiment are examples of discriminative AI.
Fine-tune and transfer learning	A process in which deep learning models can be specialized for a specific task while still maintaining knowledge from their initial training. For example, one can use an LLM for the specific purpose of classifying social media posts as discussing elections by fine-tuning it with a labelled data set of posts that do and do not discuss elections.
Generative AI	Refers to a subset of machine learning where models are used to generate content, often text, video or audio. LLMs used as chatbots are examples of generative AI.
Interpretability	Refers to people's ability to understand how a model makes decisions. For example, linear regression is a generally interpretable model, as one can easily understand the coefficients the model applies to each factor. With a multilayered neural network, on the other hand, it is much harder to interpret why specific inputs lead to the corresponding outputs.
Large language models	Refers to recent deep learning advances in the field of natural language processing, mostly due to the development of transformer architecture, which has resulted in models trained on large swathes of text. LLMs, such as ChatGPT, LLaMA and Gemini, can be used for generating, interpreting and classifying text.
LLM hallucination	Describes the tendency for many LLMs to confidently make up information in response to text queries.

Term	Explanation
Machine learning	Used to describe more recently developed technical methods such as neural networks, transformers and boosting/bagging methods. In many cases these methods are used for prediction, which involves making decisions based on data rather than explaining previous data.
Supervised learning	A subset of machine learning where training data sets are labelled such that the model is learning to associate inputs with specific outputs. An example would be developing a model to convert handwriting to text by training it with a data set of handwriting samples and their text equivalents.
Traditional statistical methods	Used to describe long-used statistical methods such as linear and logistic regressions. In many cases these methods have been used for inference, or formalizing the understanding of data.
Unsupervised learning	A subset of machine learning where training data are unlabelled, and the goal of the model is to find patterns in the data. An example would be developing a model that groups together similar handwriting samples.

About the author

Prathm Juneja is a PhD candidate and Rhodes Scholar at the University of Oxford's Internet Institute, where his primary work examines the role AI and other digital technologies can play in improving the function of, access to and equity of elections. His other research has touched on AI ethics, technology policy, machine learning and voting behaviour. Prathm regularly advises companies, organizers, governments and political campaigns on AI use, technology policy and the politics of technology.

About International IDEA

The International Institute for Democracy and Electoral Assistance (International IDEA) is an intergovernmental organization with 35 Member States founded in 1995, with a mandate to support sustainable democracy worldwide.

WHAT WE DO

We develop policy-friendly research related to elections, parliaments, constitutions, digitalization, climate change, inclusion and political representation, all under the umbrella of the UN Sustainable Development Goals. We assess the performance of democracies around the world through our unique Global State of Democracy Indices and Democracy Tracker.

We provide capacity development and expert advice to democratic actors including governments, parliaments, election officials and civil society. We develop tools and publish databases, books and primers in several languages on topics ranging from voter turnout to gender quotas.

We bring states and non-state actors together for dialogues and lesson sharing. We stand up and speak out to promote and protect democracy worldwide.

WHERE WE WORK

Our headquarters is in Stockholm, and we have regional and country offices in Africa, Asia and the Pacific, Europe, and Latin America and the Caribbean. International IDEA is a Permanent Observer to the United Nations and is accredited to European Union institutions.

OUR PUBLICATIONS AND DATABASES

We have a catalogue with more than 1,000 publications and over 25 databases on our website. Most of our publications can be downloaded free of charge.

<https://www.idea.int>

International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

As artificial intelligence (AI), including its potential role in influencing elections, has become an increasingly important topic, electoral management bodies have to develop plans to respond to and, in some cases, use AI to maintain free, fair and secure elections. AI is a rapidly evolving category of technologies that are largely unregulated, and very little research has been conducted so far concerning its potential impact on elections.

This Report is aimed at supporting electoral management bodies and other relevant parties in developing a broad understanding of the opportunities, challenges and legal implications of the use of AI for elections.

ISBN: 978-91-7671-764-6 (PDF)