



ENABLING SECURE
DEMOCRATIC ECOSYSTEMS
THROUGH AI

OCTOBER
2024

CONTENTS

ABSTRACT	3
<hr/>	
INTRODUCTION	4
Report Rational	5
<hr/>	
CURRENT STATE	7
Scoping Artificial Intelligence	7
Threats to the Democratic Ecosystem	9
<hr/>	
MAPPING A DEMOCRACY ECOSYSTEM	11
Electoral System	13
Representational System	16
<hr/>	
OPPORTUNITIES FOR AI	18
Electoral System	19
Representational System	21
<hr/>	
IMPLEMENTING AI	22
Social, Technical, and Geopolitical Trust	22
Regulatory Approach	25
Organisational Integration	28
<hr/>	
CONCLUSION	29
Recommendations	30
<hr/>	
REFERENCES	31

ABSTRACT

This report explores how AI systems can enable more secure, resilient and trusted *democratic ecosystems*. There have been numerous reported incidents of attempts to disrupt the security and resilience of digital technologies used in, and by, democratic ecosystems to reduce trust, most infamously in the US 2016 Presidential election. Recent attention has focused on how advancements in AI systems, particularly generative AI, undermine democracies through mis and disinformation. However, AI can also enable democracies to secure their ecosystems as well as provide opportunities.

This paper examines two aspects of a democracy ecosystem: electoral and representative systems. For each, this report explores how an attention of AI's capacity to improve cybersecurity offers opportunities for democratic societies. It:

- 1.** assesses the current state;
- 2.** maps two key systems of the democratic ecosystem using India and the United States as cases;
- 3.** examines opportunities AI offers to protect and enable democratic infrastructures across elections and representation;
- 4.** analyses implementation; and
- 5.** provides a series of recommendations for states to integrate AI to improve the cybersecurity of democratic ecosystems.

WRITTEN BY
ANDREW C. DWYER AND
ROXANA RADU

INTRODUCTION



The risk of artificial intelligence (AI) to democracies has generated sustained commentary and research¹. Since the launch of OpenAI's ChatGPT generative AI model and interface in 2022², significant policy attention has centred on the risk of generative forms of AI to democracies through their potential to generate content—whether text, images, audio, or video—for mis- and disinformation campaigns³. Analysis of the large number of democratic elections internationally between January and September 2024 has broadly concluded that AI-generated content has not significantly influenced outcomes⁴, supporting arguments that have sought to reduce the 'hype' around electoral disinformation arising from hacks⁵. Generative AI is only one branch of a broader suite of AI systems—commonly consisting of various machine learning algorithms—that democracies must address. Alongside AI systems, the impact of cyber operations by adversarial states to undermine trust in democratic ecosystems is not new⁶. Gaining access to compromising or confidential information can sustain misinformation and disinformation campaigns as well as directly disrupt democratic practice and engagement. The additional potential for the use of AI-supported and enabled cyber operations also pose future challenges for democracies, even if in the short-term this presents a lower risk⁷.

Despite significant contemporary research on the risk of AI to democracy, this report instead focuses on how AI can enable *secure, resilient, and trusted democracy*.

Cybersecurity, we argue, must be at the centre of all democratic ecosystems to ensure the continued trust required for open societies.

1 Manheim and Kaplan, 'Artificial Intelligence: Risks to Privacy and Democracy'.

2 OpenAI, 'Introducing ChatGPT'.

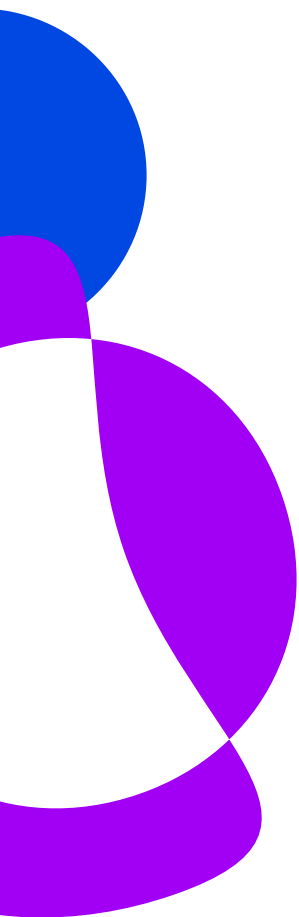
3 Heibert, 'Generative AI Risks Further Atomizing Democratic Societies'; Stockwell, 'AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections'; Janjeva et al., 'Evaluating Malicious Generative AI Capabilities: Understanding Inflection Points in Risk'.

4 Simon, McBride, and Altay, 'AI's Impact on Elections Is Being Overblown'.

5 Wilde, 'The Misguided Emphasis on U.S. Political Campaign Hacks'.

6 Whyte, 'Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare'.

7 NCSC Assessment, 'The Near-Term Impact of AI on the Cyber Threat'.






We use democratic ecosystems to refer to the broader supporting infrastructures, actors, institutions, and processes that enable the building of trust within democracy—both social and technical—embracing ongoing work within cybersecurity that seeks to examine how to build better communities and embrace cybersecurity’s capabilities for opportunity⁸. AI systems can be leveraged for greater security and resilience but must be balanced with the opportunities for citizens within democracies to partake in the ecosystem to build trust and confidence in the broader ecosystem.

To do so, we discuss a range of indicative AI use cases for democracies to consider to improve their capacity to respond to cybersecurity risk; and offer opportunities to develop trust as the core purpose of improving resilience through cybersecurity. We develop an abstracted mapping of the democratic ecosystem that has wide applicability to most states internationally. The mapping in turn establishes key actors and processes where AI could be used to enhance democratic processes. We then detail the most promising of AI use cases and reflect on the tensions of integrating AI systems into democratic ecosystems.

REPORT RATIONAL

This report examines two core building blocks for all democracies: electoral and representative systems. Electoral systems are well-researched within academic and policy literature⁹. However, representational systems—broadly incorporating how the main deliberative aspects of democracy are translated into democratic outcomes, such as through parliamentary voting—are often given less policy attention and detail.

We therefore have three aims:

1.  To review the role of AI systems in enabling secure and resilient democratic ecosystems;
2.  To map and provide recommendations for AI use in to build both resilience and opportunities in democracies, and
3.  To assess how AI can be implemented to improve trust in diverse democratic ecosystems.

⁸ Coles-Kemp and Hansen, 'Walking the Line: The Everyday Security Ties That Bind'.

⁹ Garnett and James, 'Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity'.



This report uses two of the world’s largest democracies—*India* and the *United States*—as cases to explore the opportunities that AI systems offer to secure democracy.

Both countries are geographically large, have diverse populations, secular written constitutions, and a federalised system. They both, in various ways, use electronic voting and have a bicameral legislature with elected representatives. Both countries also have significant geopolitical importance, where the democratic functioning of each is important to their respective regions and internationally.

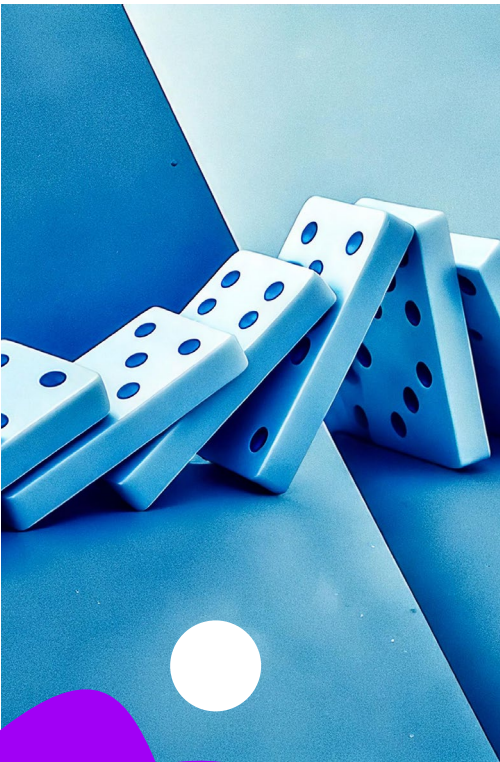
The two countries have different histories of democratic governance and economic development. The United States has evolved around its constitution written in 1787, whereas India’s contemporary system began with the post-independence constitution in 1950. Economic differences are significant: in 2024 the GDP per capita in the world’s most populous country (1.4 billion people) is \$2,484 USD, while in the United States, it stands at \$81,695 USD¹⁰. In line with the global trend of democratic recession, the quality of democracy in both India and the US has been dropping in international indices. The Economist Intelligence Unit classifies them as “flawed democracies”¹¹. Against this background, AI systems offer new opportunities to revive and enhance democratic participation, bridging the gap between access to advanced technology and public decision-making.

¹⁰ 'GDP per Capita (Current US\$)'.

¹¹ Economist Intelligence, 'Democracy Index 2023: Age of Conflict'.

CURRENT STATE

AI systems are used to secure democratic systems and processes as much as to both intentionally—and unintentionally—undermine trust in democracy. A range of automation technologies have been used extensively within cybersecurity for decades to limit malicious activity on digital systems and networks. Spam, malware, and phishing detection, vulnerability monitoring and threat analysis and prediction, asset classification and dynamic network configuration are increasingly reliant on AI systems for optimisation¹². This means that there is a backbone of AI use for security and resilience already present in many democratic ecosystems. In this section, we examine further how AI has been used in both electoral and representational systems as well as the threats and risks that AI poses to the cybersecurity of the democratic ecosystem.



■ SCOPING ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) refers to a wide range of different digital techniques and processes that allow a machine to infer on some properties¹³, which have been variously referred to as machine learning, deep learning¹⁴, and by others as potentially leading to ‘Artificial General Intelligence’ (AGI)¹⁵.

This report does not seek to provide a comprehensive definition of what ‘AI’ is nor of the contested futures of its use, but we rather engage with ‘AI systems’ to refer to the growing range of techniques and processes to develop technologies and their integration into contemporary socio-technical life, such as large language models (LLMs) that have become a dominant feature of debate on generative AI. We then use the term ‘ecosystem’ to, depending on the context, refer to the wider organisational, political, social, or other ecosystem in which AI systems are designed, developed, deployed, and utilised. In this report, we focus on the complex role that AI systems play in

12 Kaur, Gabrijelčič, and Klobučar, ‘Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions’.

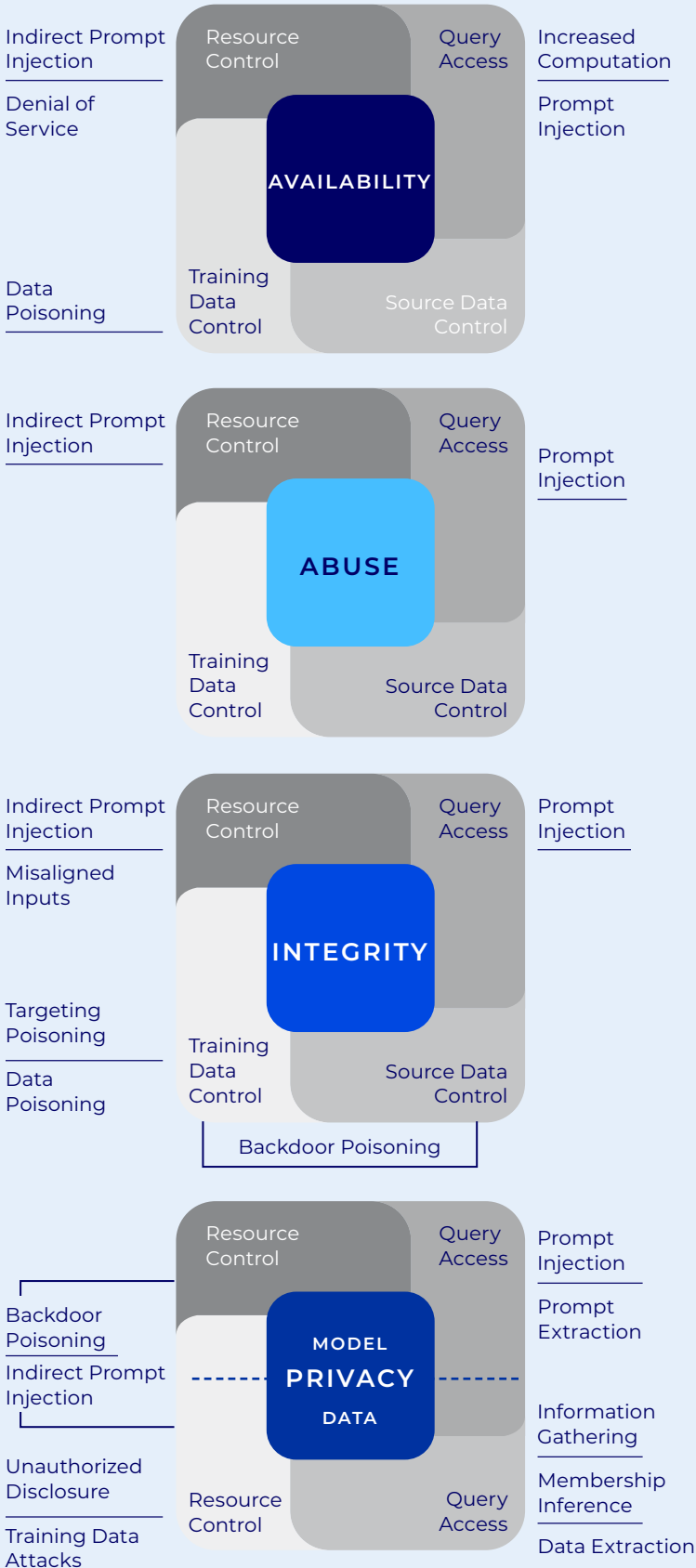
13 For example, the OECD has produced the following definition, ‘An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.’ Grobelnik, Perset, and Russell, ‘What Is AI? Can You Make a Clear Distinction between AI and Non-AI Systems?’

14 For more detail on definitions, see Manning, ‘Artificial Intelligence Definitions’.

15 McLean et al., ‘The Risks Associated with Artificial General Intelligence: A Systematic Review’.

FIGURE 1: Taxonomy of attacks on generative AI systems—adopted by the US National Institute for Standards and Technology (NIST).

Source: Vassilev et al. (2024).



both limiting cyber activity against democracies and strengthening ecosystem practices and processes to allow for better electoral and representational engagement.

There is extensive research on the risks of AI to democratic modes of governing; whether in the bias that AI encodes and reproduces or how AI is generative of new relationships and associations that may not be conducive to democratic forms of transparency and accountability¹⁶.

The latest wave of generative AI—at the root of many contemporary concerns—is itself a source of vulnerability, with training data control, query access, source code control and resource control all essential to secure.

According to Vassilev et al. (2024)¹⁷, there are at least 15 different types of attacks possible on LLMs (see Figure 1 below), each of them consequential when AI systems are integrated into key democratic functions.

¹⁶ Amore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*.

¹⁷ Vassilev et al., 'Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations'.

THREATS TO THE DEMOCRATIC ECOSYSTEM

As the NIST taxonomy of attacks against generative AI (Figure 1) indicates, neither the threats nor the techniques used against LLMs are revolutionary in form but have adapted to the context of new AI systems (e.g., prompt injection). In relation to elections and representation, AI has powered fake videos, false narratives and political manipulation around the world¹⁸. Yet, this is not something which is distinct to AI, as false media, narratives, and manipulation pre-exist AI systems' use and are assessed as having limited use by adversaries to democracy¹⁹. The ability of foreign actors to manipulate public opinion, sow discord, and undermine trust in democratic processes enhanced by generative AI models that are available for free or for low subscription fees has not significantly materialised. Interference reported in before 2024 in elections regularly noted that use of automated fake news articles, fabricated video and audio content, as well as social media bots to amplify divisive narratives, micro-targeting specific voter groups with tailored disinformation, sentiment analysis to exploit public emotions, and algorithmic manipulation to increase the visibility of polarising or misleading content. Such uses against democratic ecosystems have continued to be the dominant theme in 2024²⁰, rather than uses that increase the scale, speed, or production of mis- and disinformation according to an OpenAI report²¹.

Despite the lack of evidence of AI to disrupt current democratic ecosystems, there are concerns over long-term “deep doubt”²² that AI systems may create.

Within the US, the most evident use has been by the presidential candidate, former President Trump and for other forms of political satire²³ in producing artificial content. Within India, there were no major incidents reported in relation to the elections, but there was also an active effort to preserve democratic practices and use AI in innovative ways to ensure greater access to information, such as multilingual facilitation for political communication.

18 Rest of World, 'Maduro Pledges to Cede Power in Faked Video'.

19 Nimmo and Flossman, 'Influence and Cyber Operations: An Update'.

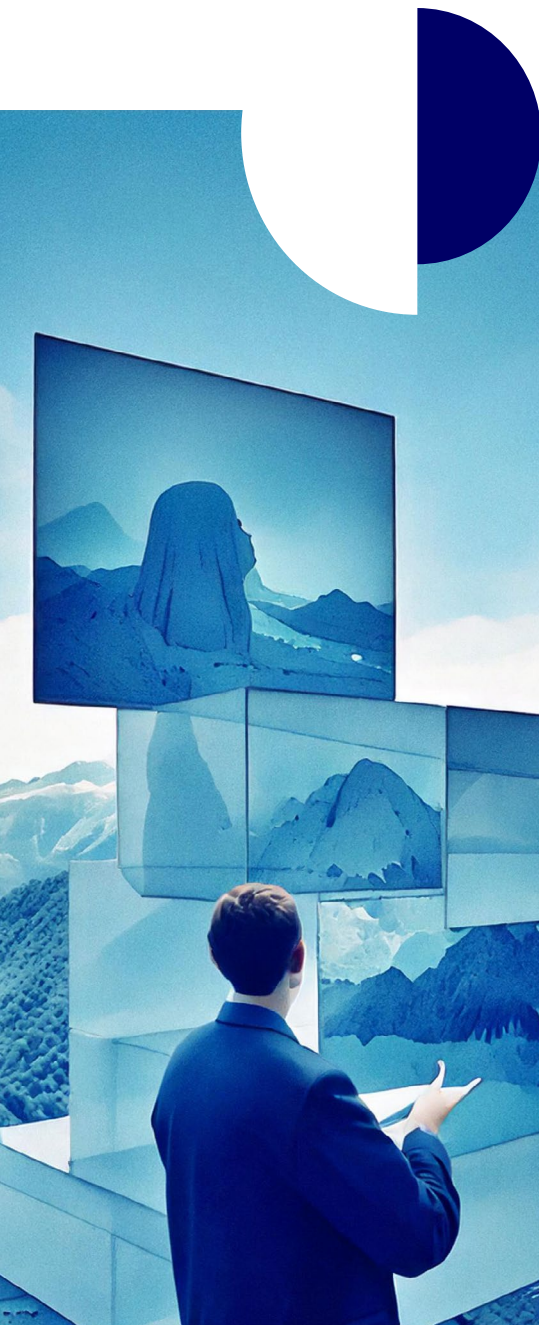
20 Thornhill, 'Deepfakes Pose a Particular Threat, but They Are Not as Dangerous as You Think'; Rebelo, 'India's Generative AI Election Pilot Shows Artificial Intelligence in Campaigns Is Here to Stay'.

21 Nimmo and Flossman, 'Influence and Cyber Operations: An Update'.

22 Edwards, 'Due to AI Fakes, the “Deep Doubt” Era Is Here'.

23 Robins-Early, 'Trump Posts Deepfakes of Swift, Harris and Musk in Effort to Shore up Support'.

An opportunity and space for democracies to build AI systems that enable secure, resilient, and trusted democratic ecosystems.



The real impact of AI-generated content is difficult to estimate, as some of it received little engagement. However, the effort to distinguish ‘authentic’ content can be difficult. For instance, a video showing swapped Indian parliamentary seat numbers was wrongly deemed to be AI-generated²⁴. For Shukla and Schneider, in the 2024 Indian election, AI was a *net positive for democracy*²⁵. AI tools later supported canvassing and political campaigning, personalised messages and emotional appeals for voter persuasion, widely distributed on WhatsApp and on social media. AI voice cloning became widespread, but deep fakes were not as common as initially expected²⁶. In an unprecedented move, in the southern state of Tamil Nadu, AI was also leveraged to bring back deceased influential figures on social media as an emotive tactic²⁷, mobilising both an elderly electorate likely to respond to the appeal and a younger one enticed by its novelty, in a cultural environment in which “nobody speaks ill of the dead”.²⁸

For cybersecurity of critical systems for democracy, there have been in hacks in the US against voter election rolls²⁹ and political parties by countries such as Iran³⁰ and Russia³¹, as well as sensitive healthcare records of members of the US Congress³². Whilst in India, there have been persistent concerns and claims of attacks against the use of voting machines³³ but fewer confirmed reports of direct cyber-attacks and intrusions. Whether hacking of political parties, for instance, has a significant direct effect on democratic outcomes is highly contested³⁴, but overall disruptions to trust in democratic ecosystems is harder to measure. Yet, there is no conclusive evidence that AI is being used—beyond the production of phishing messages—to enhance conventional cyber operations by states. This provides an opportunity and space for democracies to build AI systems that enable *secure, resilient, and trusted democratic ecosystems*.

24 Nisos, ‘What India’s Elections Can Teach Us About AI’.

25 Shukla and Schneider, ‘Indian Election Was Awash in Deepfakes—but AI Was a Net Positive for Democracy’.

26 Rebelo, ‘India’s Generative AI Election Pilot Shows Artificial Intelligence in Campaigns Is Here to Stay’.

27 Pasricha, ‘AI, Deepfakes, Social Media Influencers—India’s Mammoth Election Sees It All’.

28 Dutt, ‘Indian Politicians Are Bringing the Dead on the Campaign Trail, with Help from AI’.

29 Sampathkumar, ‘US Cyber Security Official Says 21 States’ Voter Rolls Were Hacked during 2016 Election’.

30 Office of Public Affairs, ‘Three IRGC Cyber Actors Indicted for “Hack-and-Leak” Operation Designed to Influence the 2024 U.S. Presidential Election’.

31 Office of the Director of National Intelligence, ‘Assessing Russian Activities and Intentions in Recent US Elections’.

32 Associated Press, ‘Sensitive Personal Data of US House and Senate Members Hacked, Offered for Sale’.

33 Biswas, ‘India Election 2019: Are Fears of a Mass Hack Credible?’

34 Frankovic, ‘Russia’s Impact on the Election Seen through Partisan Eyes’.

MAPPING A DEMOCRACY ECOSYSTEM

Democracies are exceptionally varied whether culturally, politically, institutionally, economically, and beyond according to their distinct histories, compromises, and geopolitical relationships. This plurality in democratic practice in turn shapes the infrastructures and systems that countries deploy and use. This dynamic democratic ecosystem in turn requires that AI systems must be adapted to secure systems, increase resilience and offer opportunities to build trust. This report details two key elements, the **electoral** and **representational** systems. These present two key aspects to all democracies, in how people vote for their representatives and how those representatives conduct their business. We define the two systems thus:



Electoral System

The infrastructure that supports the democratic expression of a community through providing capacity for the administration, delivery, and implementation of a vote.



Representational System

The infrastructure that supports the democratic implementation and negotiation of policies among elected representatives, typically through an institution such as a parliament.

Each of these systems are key targets for adversaries in which to undermine confidence and trust within states and their associated democracies. For both systems, we exclusively refer to their enactment at the national or federal level of the state, and do not explicitly refer to regional, local, or community-centred forms of democracy. There are many forms of democracy that this in turn pays less attention to, including deliberative forums, civil dialogue, and other non-state expressions of democracy. This is to provide a narrower scope whereby we can offer more focused recommendations across democratic ecosystems applicable to multiple states. Through our selected cases of India and the United States, we intend to provide a basis to consider how other states may consider the use of AI systems. In turn, we intend to provide forums, dialogues, and communities opportunities to build upon this report to examine

how AI systems may build more secure, resilient, and trusted democracy for their needs. We identify a range of key actors across the democratic ecosystem: within the electoral system, *election management* bodies who administer elections, and the *election technology industry* that produces a range of digital technologies required for elections (e.g., voting machines, databases for electoral rolls). With the representational system, there is the legislature itself (e.g., a parliament) who is responsible for securing the activities of the representative decision-making process. Across these two systems, as part of the broader democratic ecosystem are political parties, the media, representatives, and citizens. These are only an indicative sample of actors: civil society, communities, business, and other interests all have a role to play but will vary according to each state.

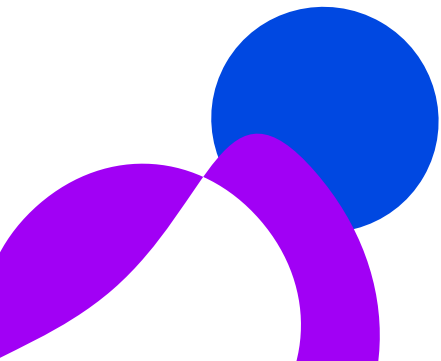
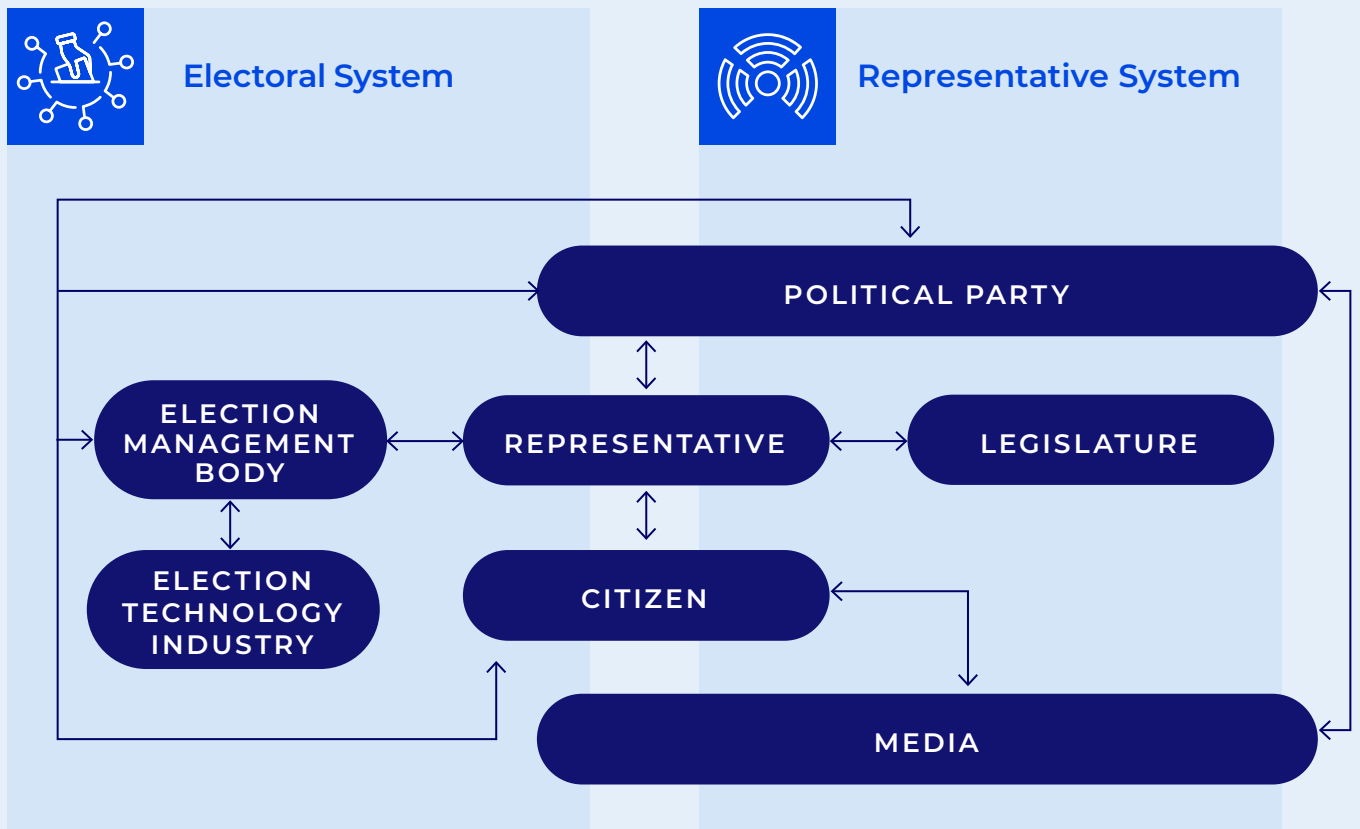


FIGURE 2:

An overview of our typology of an abstracted democracy ecosystem, with the main actors and institutions for both electoral and representational systems.





ELECTORAL SYSTEM

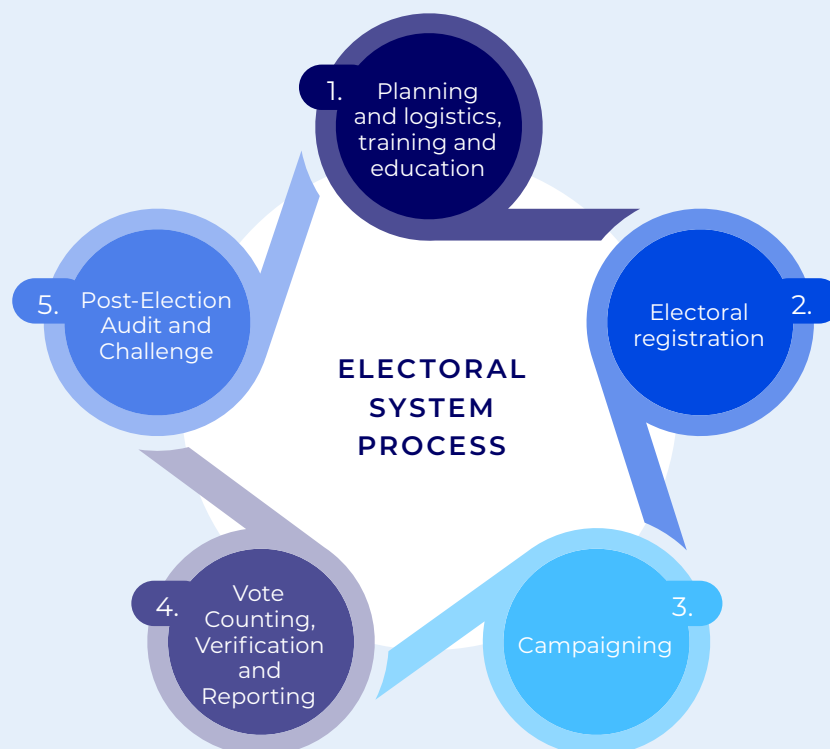
The cybersecurity of electoral systems has been widely covered in prior research³⁵, yet the adoption of AI in electoral processes remains extremely limited³⁶, in large part due to the challenges involved in maintaining the integrity of the electoral process and the systems used³⁷. However, there are areas where AI systems can aid the electoral system.

We engage with Brown et al.’s³⁸ classification of the electoral process, outlining five key elements relevant to cybersecurity:

1. Planning and logistics, training and education;
2. Electoral registration;
3. Campaign regulation;
4. Vote counting, verification and reporting; and
5. Post-election audit and challenge.

FIGURE 3:

An abstracted outline of the electoral system process.



35 Chaudhary, Chanussot, and Wally, 'Understanding Cybersecurity Throughout the Electoral Process: A Reference Document'.

36 Martin, 'Deepfakes Are Here and Can Be Dangerous, but Ignore the Alarmists—They Won't Harm Our Elections'.

37 Padmanabhan, Simoes, and MacCarthaigh, 'AI and Core Electoral Processes: Mapping the Horizons'.

38 Brown et al., 'Cybersecurity for Elections: A Commonwealth Guide on Best Practice', 26.



We expand beyond their focus on electoral management bodies (EMBs) to consider the broader democratic ecosystem as presented in Figure 2 to include political parties and the media in sustaining democratic practice with regards to electoral systems.³⁹ This is essential as a lack of effective cybersecurity within these actors has the potential to reduce trust and confidence in democracy. For both India⁴⁰ and the United States⁴¹ there are set terms for elections albeit with elections being conducted over a longer period⁴². The extended period of voting means that the threat to cybersecurity extends to those actors who are reporting and campaigning in addition to a focus on election ‘events’ that occur only on one day. In Table 1, we detail each stage, including the main actors from our mapping exercise and an indicative description.

³⁹ We do not include social media in our analysis, as another paper within this collection already considered extensively the use of AI within this element of the democracy ecosystem. See Ramaciotti, ‘Depolarizing and Moderating Social Media with AI’.

⁴⁰ In India, the Lok Sabha (the lower house of the Indian Parliament) is the directly elected ‘House of the People’ every five years. There is no direct election to the upper house (Rajya Sabha) as members are elected from the State or Union Territory legislatures or appointed by the President, which are excluded from this report. The President is elected through an electoral college of the Houses of Parliament, Legislative Assemblies of States and the Union Territories of Delhi and Pondicherry and is therefore also excluded.

⁴¹ In the United States, Congress is directly elected, with all members of the House of Representatives elected every 2 years, and members of the Senate elected every 6 years, staggered every 2 years with a third of members up for election. The President is elected every 4 years, but this is not directly elected, and is instead elected by an Electoral College, guided by a popular vote. This is therefore included in the report’s analysis.

⁴² For example, in the US, mail-in ballots and early voting means that there is a sustained period of voting in the electoral system.



TABLE 1:

Overview of the main stages and actors of electoral systems.

Electoral System Component	Principal Actors	Brief Description
<p>PLANNING AND LOGISTICS, TRAINING AND EDUCATION</p>	<p>Citizen; Election Management Body; Election Technology Industry; Media Political Party</p>	<p>Each actor will have different plans in advance of an election. This includes creating systems and maintaining technology for the enactment of the vote by the election technology industry (e.g., voting machines), the logistics of holding a vote and how communications may be handled, as well as ensuring education and training around how to conduct the election by the election management body to personnel as well as citizens. For political parties, this will be to ensure that there are effective policies to be voted upon, and the media preparing infrastructure, contacts and content for publishing before an election is called.</p>
<p>ELECTORAL REGISTRATION</p>	<p>Citizen; Election Management Body; Political Party; Representative</p>	<p>Registrations must take place with the election management body. Most commonly this is a citizen registering to vote, but there will also be registrations by representatives and political parties according to the electoral system used within a country.</p>
<p>CAMPAIGNING</p>	<p>Media; Political Party; Representative</p>	<p>In contrast to ‘campaign regulation’ of Brown et al., we take a wider view of campaigning to include how political parties communicate their message and how the media report on the election. Representatives may wish to distribute campaigning material to citizens.</p>
<p>VOTE COUNTING, VERIFICATION AND REPORTING</p>	<p>Election Management Body; Election Technology Industry; Media</p>	<p>For the election management body, the processing of vote during an election is their primary role. However, for some elections that use digital processes, the election technology industry will play a significant role (especially if there are concerns about processes during an election voting period). Likewise, the media are an essential medium to communicate and disseminate results.</p>
<p>POST-ELECTION AUDIT AND CHALLENGE</p>	<p>Election Management Body; Election Technology Industry; Media; Representative</p>	<p>After an election, there will need to be an audit of the election as well as potential challenges made concerning the management of the election. This could include recounts and technical audits of the election technology.</p>

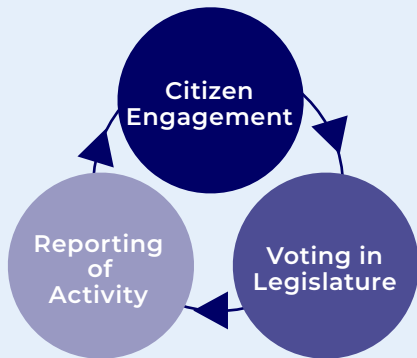
Together, these five elements of the electoral system detail the range of processes and actors involved in elections. Much focus on election security stresses the ‘act’ of voting (i.e., vote counting, verification and reporting). However, by examining the broader democracy ecosystem, we can see how a wider range of actors and processes must be considered in cybersecurity.



REPRESENTATIONAL SYSTEM

FIGURE 3:

An abstracted outline of the representational system process.



The cybersecurity of representational systems—broadly consisting of legislative activity—is largely understudied and rarely in connection to secure democratic ecosystems. However, there are resources for legislatures to improve their cybersecurity⁴³ and there are a range of initiatives that help legislatures in sharing best practice of AI use⁴⁴.

In Table 2, we detail each stage, including the main actors from our mapping exercise and an indicative description.

TABLE 2:

Overview of the main stages and actors of representational systems.

Representational System Component	Main Actors	Brief Description
CITIZEN ENGAGEMENT	Citizen; Legislature; Media; Political Party; Representative	Engagement between citizens and their representatives is a key element to representative democracies. Much of this direct interaction between representatives (including their offices) and citizens occurs through digital technologies often using the legislature’s IT systems, whether by email and online appointments. Likewise, political parties wish to promote their messages about current democratic activity, which the media may report and investigate.
VOTING IN LEGISLATURE	Legislature; Political Party; Representative	One of the key responsibilities for a representative is to participate in the activities of the legislature; this may be through voting on laws, sitting on committees, as well as other relevant activities. In some states, this is supported through digital technologies providing capabilities to aid the voting process in a legislature.
REPORTING OF ACTIVITY	Citizen; Media; Representative	Beyond citizen engagement, the media may wish to report and investigate activities of government, contemporary affairs, or any other relevant information. This is a crucial aspect to a representative system, offering a diversity of perspectives that inform citizens as well as representatives. In turn, citizens and representatives are informed during the democratic process and can present campaigns to influence the democratic process.

⁴³ Summers, Moulton, and Doten, 'Cybersecurity Handbook for Parliaments'.

⁴⁴ Fistsilis, von Lucke, and De Vrieze, 'Guidelines for AI in Parliaments'.



Across the democracy ecosystem, we have mapped a high-level typology consisting of seven key processes and seven principal actors within the system that are applicable to most democracies (see summary in Table 3).

In the next section, we develop what opportunities for AI exist across the democratic ecosystem before discussing how these may work in our cases of India and the US.

TABLE 3:

An overview of the mapping between the democratic ecosystem's components and main actors.

	DEMOCRACY ECOSYSTEM COMPONENT	ACTOR						
		Citizen	Election Management Body	Election Technology Industry	Legislature	Media	Political Party	Representative
ELECTORAL SYSTEM	Planning and logistics, training and education	X	X	X		X	X	
	Electoral Registration	X	X				X	X
	Campaigning					X	X	X
	Vote Counting, Verification, and Reporting		X	X		X		
	Post-Election Audit and Challenges		X	X		X		
REPRESENTATIONAL SYSTEM	Citizen Engagement	X			X	X	X	X
	Legislature				X		X	X
	Reporting of Activity	X				X	X	X

OPPORTUNITIES FOR AI



There are a range of opportunities for AI to enhance security, resilience and trust within the democratic ecosystem. For most parts of the democratic system, a core benefit of AI technologies will be the monitoring and detection of threats. The use of AI technologies has become a commonplace, often 'additional' feature of many cybersecurity vendors' endpoint and network solutions. AI-enabled cybersecurity products can offer significant improvements, especially on IT systems, extending to websites, databases, and email by offering identification and detection of 'unseen' malicious techniques and processes. This includes a range of AI systems, including machine learning to recognise patterns, behavioural analytics to analyse anomalies, to automatically detecting new threats⁴⁵.

Due to the growing scale and speed of malicious actors' capabilities, integrating a range of AI-enabled monitoring and detection should form a bedrock for the use of AI across the democratic ecosystem.

However, this for operational technology (OT), for example voting machines, it is likely that these should not have a third-party installed on these, and India's voting machines would not be able to load such cybersecurity products, meaning there must be a careful assessment of the risk that we explore more in the next section. For the remainder of this section, we highlight some key opportunities for using AI systems across the democratic ecosystem.

⁴⁵ Kaur, Gabrijelčič, and Klobučar, 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions'; Dwyer, 'The Recursive, Geopolitical, and Infrastructural Expertise of Malware Analysis and Detection'.



ELECTORAL SYSTEM

1.

PROCURING SECURE SYSTEMS FOR POLITICAL PARTIES

Political parties frequently manage large volumes of sensitive data essential to data-driven campaigns. This information may include voter profiles but also donor lists, policy strategies, and other confidential material essential for creating targeted and effective outreach. The handling of this data often involves a diverse range of actors, including campaign staff, consultants, and third-party vendors, which can complicate oversight and security. Given the decentralised nature of campaigns and requirements to access IT systems, sensitive information can be accessed by multiple individuals across different platforms, increasing the risk of unauthorized access or data breaches. Here, detecting unusual behaviour can be aided through patterns detected by machine learning, which may learn from other indicators of compromise and infer similar behaviours, compared to human-written rules. For example, unusual patterns of email behaviour—such as from phishing—are more likely to be detected, which would aid political parties to identify suspicious behaviour and limit leaks of information (as was the case in the US 2016 DNC hack where an email was inadvertently marked as legitimate by an aide⁴⁶). This information is collated over many years and comes from a range of sources. For example, in the UK, its Labour Party had a breach of its systems which could have led to automated harvesting of voter information⁴⁷.

2.

VERIFYING THE ELECTORAL ROLL

One of the biggest tasks in democracy is ensuring that citizens have a right to vote and that it can be secure, resilient, and trusted. Matching algorithms can be used to supplement conventional methods of verification of rolls to avoid duplication, as well as using other state-held data about residency as well as those that may not appear to be registered. By enhancing the integrity of the electoral roll using AI systems—for example to avoid multiple registrations—could increase the overall resilience of the electoral process and offer opportunities to ensure those who are not registered are identified. For example, these AI systems are already being used in the United States⁴⁸.

46 Harding, 'Top Democrat's Emails Hacked by Russia after Aide Made Typo, Investigation Finds'.

47 Crerar, 'Labour Glitch Put Voting Intentions Data of Millions at Risk'.

48 The Electronic Registration Information Center (ERIC), <https://ericstates.org/>



ELECTORAL SYSTEM

3.

SECURING VOTING MACHINES

Concerns about the security of voting machines and vote-counting systems have become a significant issue in discussions on electoral process integrity worldwide. The potential risks include the infiltration or manipulation of these systems to alter vote counts, disrupt the tallying process, or undermine trust in the legitimacy of election results. In many countries, fragmented election infrastructures, where different regions or municipalities use varied technologies and software, raise concerns about inconsistent security measures and uneven protections against cyber threats⁴⁹. Additionally, outdated voting technology in some regions increases the vulnerability to hacking, while machines without paper backups complicate efforts to verify electronic votes in the event of a cyberattack or technical failure, jeopardizing the credibility of the election process. AI systems, such as behavioural analytics, can be used to analyse any anomalous behaviour to improve the integrity and security of the systems. These will need to be tailored to the type of voting technology used. In India, however, the voting machines would be unable to use these AI systems directly due to the significant hardware limitations of the devices.

4.

VALIDATING VOTER COUNTS

Counting of votes can be a complex process. In India, the use of electronic voting machines across the entire country as well as a 'voter verifiable paper audit trail' (VVPAT) enable citizens to view a paper confirmation of their vote. A selection of these are then used to manually validate the electronic counts in counting centres. Likewise, mail-in ballots frequently have signatures which are provided to the electoral management body that require signatures to be compared to validate that the vote has been authorised by the voter. Manual inspection of voter records can be time-consuming and expensive, with pressure to often do counting quickly and efficiently. In this case, using AI image recognition capabilities to supplement the audit of VVPAT in the case of India or signatures in mail-in ballots, allows a complementary resource to allow democracies to add an additional layer of verification to both ballot and some voting machine counts.

⁴⁹ Chaudhary, Chanussot, and Wally, 'Understanding Cybersecurity Throughout the Electoral Process: A Reference Document'.



REPRESENTATIONAL SYSTEM

1.

CITIZEN ENGAGEMENT

Many representatives receive a high number of engagements with constituents—but also those who may wish to artificially skew engagements, in the case of e-petitions, for example. Using machine learning pattern recognition as well as threat information, it is possible to reduce the likelihood of malicious engagement and limit phishing attempts. AI systems, particularly using natural language processing and generative AI, could be an opportunity to centre attention on citizen’s priorities, providing summarisation and personalised feedback following public submissions. Moreover, AI-based tools could support new forms of engagement with representatives. For example, the “AI Steve” chatbox was used as a campaign platform by one candidate in the UK 2024 general election, where local validators screened policy proposals received online and added them to the manifesto when they passed a 50% support threshold⁵⁰. Therefore, being able to give greater trust to representatives and their supporting offices by improving the ability to identify malicious forms of engagement allows for more possibilities to use open tools that benefit representational systems.

2.

COMBATING ADVERSARIAL ACTIVITY

Conventional AI monitoring and detection is unlikely to be sufficient for legislatures, who are high priority targets for adversaries. AI systems utilising significant threat intelligence data and patterns across a legislature could build up contextual awareness of hacks and influence campaigns to build patterns that may show adversarial activities. This would require deep access to representative’s systems, necessitating significant trust that authorities are independent and will not seek to use that information to undermine the representational system. Countries such as the UK have prioritised internal government coordination to protect democratic integrity from threats of external interference, setting up groups such as the Defending Democracy Taskforce, created in November 2022⁵¹. As it transpired later, the country’s democratic institutions had been targeted by state-sponsored cyber operations between 2021 and 2022, with various levels of success⁵². While no parliamentary accounts were breached, the UK Electoral Commission was compromised⁵³.

50 Davis, ‘Meet AI Steve: The Bot-Driven Politician Using Artificial Intelligence on the Campaign Trail’.

51 UK Government, ‘Ministerial Taskforce Meets to Tackle State Threats to UK Democracy’.

52 UK Government, ‘UK Holds China State-Affiliated Organisations and Individuals Responsible for Malicious Cyber Activity’.

53 The Electoral Commission, ‘Information about the Cyber-Attack’.

IMPLEMENTING AI



Ensuring that AI provides opportunities for the broader democratic system requires an assessment of how to appropriately implement various technologies according to their organisational integration, their trust frameworks, and capabilities.

■ SOCIAL, TECHNICAL, AND GEOPOLITICAL TRUST

It is highly unlikely that most actors in the democratic ecosystem will build their own AI systems. This means that there are important trust relationships that those responsible for managing both electoral and representational systems must navigate, build, and secure.

As AI systems often require highly technical skills to build and maintain, especially with machine learning models, 'foundational' models are likely to be widely used for security.

Adaptations to 'fine tune' such models will continue. For most of the democratic ecosystem, it is then not the actors who build, or even fine tune, the AI systems that are required to tackle the threat of AI-supported and enabled intrusions into the future.

This means that there are questions around the supply chain for the implementation of AI systems. For the USA, which is home to many of the largest AI companies who are subject to the US's regulatory pressures, this is likely to be a less complex problem that it will be for other states, such as India, who are likely to be customers of such AI systems and their integration into their democratic ecosystems. As much as AI systems may be able to increasingly provide automated and effective monitoring and detection of threats to systems, there is a trust relationship between the supplier and customer.



The 2024 CrowdStrike incident demonstrates some of the risks of implementing AI without understanding the complex dynamics of the infrastructure that supports the deployment of AI systems. In this case, CrowdStrike sent an update to its Falcon sensor, which provided a range of AI-supported monitoring and detection techniques, causing system crashes⁵⁴. Even though such systems are a backbone to effective cybersecurity, their integration must carefully take into account how using AI to secure and increase resilience introduces new attack vectors and vulnerability across the democratic ecosystem.

This means that it is simply not enough to view AI systems integration *within* and by actors, but across the who (eco)system due to the cascading role of risk that digital technologies introduce. Efforts in this direction have included vetted lists of providers and multi-vendor approaches. In the US, detection products from the Russian company Kaspersky have been removed from government networks due to accusations by the US of Russia using the company's tools for espionage⁵⁵, demonstrating some of the complex interdependencies about technical and geopolitical trust surrounding the integration of AI systems in cybersecurity.

54 CrowdStrike, 'External Technical Root Cause Analysis — Channel File 291'.

55 Dwyer, 'The Recursive, Geopolitical, and Infrastructural Expertise of Malware Analysis and Detection'; Office of Congressional and Public Affairs, 'Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers'.

There are also questions of algorithmic bias and how these appear⁵⁶. There has been significant work in cybersecurity that has exposed not only algorithmic bias but also inequality in access⁵⁷. With regards to election security, lack of access has been a predominant theme within the United States regarding concerns over voter suppression. There is a danger that using AI to, for example, voter registration further causes disenfranchisement if it is implemented in such a way to restrict the number of options or capacities to question the AI system. Citizens, journalists, and others must also be able to understand how and why AI is being implemented to improve resilience across the democratic system. AI systems' cybersecurity—and thus resilience and trust—in the democratic system is then fundamentally a combination between social and technical forms of trust; and one that is difficult to build but easy to degrade. Hence, the opportunities of AI systems we presented should only be used selectively and in consultation with the actors we have identified in our mapping (as well as those outside)—so that any changes are understood and crucially, widely accepted, before adoption.



56 Aradau and Blanke, 'Governing Others: Anomaly and the Algorithmic Subject of Security'; Bellanova et al., 'Toward a Critique of Algorithmic Violence'.

57 Coles-Kemp and Hansen, 'Walking the Line: The Everyday Security Ties That Bind'.at least, the connection between an individual's security needs and the protection of assets if it is to help design secure services with which citizens can safely engage. We exemplify these attributes from case studies conducted as part of two sociotechnical research projects: the UK government and research council funded Cyber Security Cartographies (CySeCa)



REGULATORY APPROACH

AI is here to stay as a general-purpose technology. The discussions on the trade-offs between opportunities and risks have matured in recent months, shifting the focus from soft law mechanisms to hard law⁵⁸. In 2024, the European region became the first to adopt legally binding rules in the form of the EU's AI Act, using a risk-based approach to categorise AI applications according to risk levels, with the highest-risk applications, like those impacting fundamental rights and democracy, facing the most stringent regulations. Moreover, the Council of Europe adopted its Framework Convention on AI and Human Rights, Democracy, and the Rule of Law, which covers the use of AI by public and private actors, for the entire lifecycle of AI systems. It sets out 7 principles, highlighting safe innovation, reliability, accountability and transparency, alongside human dignity, privacy and non-discrimination. It also specifies the remedies and procedural rights in relation to human-AI system interaction, and risk and impact management requirements. The Framework convention was negotiated by the 46 Council of Europe member states, the European Union and 11 non-member states⁵⁹, but remains open to any country. Around the world, many other jurisdictions have started the process of designing laws for the use of AI⁶⁰, including in relation to electoral integrity and algorithmic transparency.

Democracies like India are taking a cautious and piecemeal approach to regulating AI, especially in the context of elections.

India currently relies on traditional media laws and digital media regulations, such as the Information Technology Act and the Penal Code⁶¹, to govern AI-generated content like deepfakes, without having an AI-specific regulatory framework. The Indian government has tasked its policy think tank, NITI Aayog, with developing broader AI guidelines⁶², which focus on sectors like healthcare and education but do not directly address AI's role in elections. In 2023, a new privacy law, the Digital Personal Data Protection Act, was introduced, which may help address privacy concerns related to AI platforms in the years to come.

58 Radu, 'The G20 and Global AI Governance'.

59 Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America and Uruguay

60 Mulligan, 'There Are More than 120 AI Bills in Congress Right Now'.

61 Financial Express, 'The Upsides, the Downsides, and the Risks of Artificial Intelligence in Elections'.

62 National Institution for Transforming India, 'National Strategy for Artificial Intelligence'.



Meanwhile, the Election Commission of India has issued voluntary guidance for the ethical use of social media by political parties during election periods⁶³ but compliance remained hard to monitor. Enforcement deficiencies were also encountered for commitments that large social media platforms had themselves put forward, such as labelling AI-generated or synthetic content (Meta) or providing transparency over campaign spending via tools such as Meta's Ad Library or Google Ads Transparency Center.

In the United States, the Federal Election Commission (FEC) and bipartisan efforts on election security have targeted foreign influence, including AI-driven disinformation. They have also addressed transparency in online political advertising, requiring disclosure of the entities behind campaign ads. Broader frameworks, such as NIST's AI risk management⁶⁴ help guide the deployment of AI in various sectors, including in relation to information security. More specific bills combatting deepfakes and threats to political campaigns have been under consideration in 14 American states⁶⁵, building on the example of legislation passed in Texas⁶⁶ and California⁶⁷ in 2019.

But even when these state bills address the same concern, there is no harmonisation of methodology, exceptions and punishments, creating further inconsistencies for AI developers and additional space for manoeuvre for those willing to exploit them.

63 Chandak, 'Responsible and Ethical Use of Social Media Platforms and Strict Avoidance of Any Wrongful Use by Political Parties and Their Representatives during MCC Period in General Elections and Byelections-Regd', 6 May 2024.

64 NIST, 'Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile'.

65 Edelman, 'States Turn Their Attention to Regulating AI and Deepfakes as 2024 Kicks Off'.

66 Texas, An act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election.

67 Tashman, "'Malicious Deepfakes'—How California's A.B. 730 Tries (and Fails) to Address the Internet's Burgeoning Political Crisis'.

Although regulation is a crucial component for securing AI systems and ensuring adherence to higher protections standards, there is limited alignment among stakeholders and among state actors as to the priorities to be pursued. For there to be both technical and social forms of trust to ensure the resilience and opportunities that AI offers in democratic ecosystems, there must be robust regulatory and oversight mechanisms in place. At an early stage in its governance, AI suffers from a lack of agreed definitions and a wide diversity of regulatory approaches⁶⁸. Most governments remain users, not producers of AI, and the limited AI market competition shapes their regulatory space, amid growing geopolitical tensions.

Ahead of the US Presidential elections in November, both regulatory frameworks and voluntary commitments play significant roles, as do compliance and oversight. Regulatory measures establish mandatory standards for campaign finance, voter registration, and ballot security, while voluntary commitments from organizations and stakeholders enhance these efforts by promoting best practices and enhancing transparency through real-time monitoring and accessible reporting, both of which can be supported by AI tools. Independent oversight bodies leverage both avenues to monitor compliance, ensuring accountability and fostering public trust.

This dual approach not only upholds electoral integrity but also reinforces the foundations of democracy, encouraging active civic engagement.



⁶⁸ Radu, 'The Variable Geometry of AI Governance'.

■ ORGANISATIONAL INTEGRATION

We suggested earlier that the greatest immediate impact upon improving the resilience of the democratic ecosystem was the use of AI-enabled monitoring and detection technologies. There are a range of AI solutions that may be of benefit to democracy, but they must be integrated according to the sensitivities and priorities of the organisation. For example, when adopting behavioural analytics into a legislature's systems, this requires important principles of segregation of duties and independence of the Parliamentary IT services from the influence of the government of the day. This is essential to ensure that those same cybersecurity systems are then not abused by those in power.

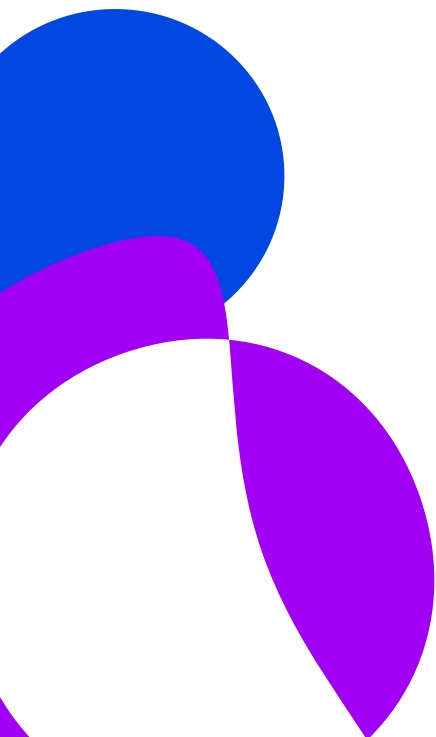
When considering the adoption of AI systems within organisations, it is essential that there are clear, and validated, organisational policies following standard cybersecurity frameworks⁶⁹ to ensure that the security controls implemented are in place, are maintained, and updated according to the objectives of, and threats to, that element of the democratic ecosystem⁷⁰.

This in turn requires a clear position on AI regulation. Like in any other area of cybersecurity, the management of its implementation and integration is key to success. Most cyber incidents occur because of poor implementation of security controls around technology. Thus, any benefit of AI in a democracy ecosystem must appropriately select not only how it may enable security, resilient, and trusted democracy, but how the AI system itself must also be secured.

⁶⁹ For example, the NIST Cybersecurity Framework or ISO/IEC 27001

⁷⁰ Orey, 'A Proposal for Bipartisan Federal Election Reform'.

CONCLUSION



AI systems have an essential role to play in enhancing the resilience of democratic ecosystems through improving cybersecurity and how this intersects with enhancing trust across democracies. Some AI system implementations may increase technical trust (e.g., facial recognition for voter authentication) that in turn decrease social trust and are thus not included as an ‘opportunity’ for enabling secure democratic ecosystems. It is at this intersection that this report seeks to find a ‘middle ground’ so that AI systems offer opportunities to enhance democracy. This report highlights the dual role of AI as both a tool for resilience—helping democracies withstand internal and external threats—and as a catalyst for engagement, opening new avenues for citizen and stakeholder participation, transparency, and innovation. The cases of India and the United States, representing different scales and complexities of democratic systems, provide a valuable comparative lens through which AI’s diverse applications can be understood.



Analysing AI’s multifaceted role at the intersection of technical and social trust, this report offered a comprehensive assessment of how advanced technologies can both protect and advance democratic processes.

Specifically, it provided a detailed evaluation of the current state of AI and its implications for democracy; it mapped and analysed two critical systems within the democratic ecosystem, discussing how AI can safeguard and strengthen electoral and representational systems; examined the practicalities and challenges involved in implementing AI solutions within democratic systems; and concludes with series of targeted recommendations for governments and policymakers.

RECOMMENDATIONS

1. **AI system integration must view the entire democratic ecosystem and its cybersecurity:**

There has been a typically narrow view of cybersecurity to secure electoral systems and, in particular, voting systems. We argue that to leverage the opportunities of AI means understanding how the broader democratic system can engage with AI. Securing with AI means not only of the technical systems, but its aim must be to build trust and confidence and not to design systems that are unusable or create additional insecurities for citizens.

2. **AI-enabled monitoring and detection software should be reasonably installed on all IT estates:**

As a foundational element to improving cybersecurity, enabling the use of AI detection on systems will become increasingly important as AI supported and enabled malicious activity becomes more prevalent. Any integration of such detection software must follow common cybersecurity practices, emphasising segregation of systems and redundancy within systems to enable continuity, even during an incident.

3. **States should map out their democracy ecosystem:**

Each country has its own unique features and attributes. This means that its democracy ecosystem is unique and thus has different pressures. This means that where AI systems can provide greater opportunities for democracy is essential for states to explore. This means engaging with all the actors—and others—that our mapping has identified.

4. **Sharing of best international practice:**

The fragmented information about democratic ecosystems should be brought together, where activity across inter-parliamentary initiatives and international electoral security come together to expose the interdependencies that are present.

5. **Aligning regulatory approaches:**

The democratic ecosystem relies on the availability of “fit-for-purpose” rules that can evolve alongside technology. The diverse visions of AI development, the lack of a common vocabulary and the absence of a harmonised assessment of risks have so far stalled progress at both the national and international level. Democratic governments need to align their regulatory approaches to ensure that safeguards for their core functions and processes are prioritised.

REFERENCES

- Amoore, Louise. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, N.C.: Duke University Press, 2020.
- Aradau, Claudia, and Tobias Blanke. 'Governing Others: Anomaly and the Algorithmic Subject of Security'. *European Journal of International Security* 3, no. 1 (2018): 1–21. <https://doi.org/10.1017/eis.2017.14>.
- Associated Press. 'Sensitive Personal Data of US House and Senate Members Hacked, Offered for Sale', 9 March 2023. <https://www.theguardian.com/us-news/2023/mar/08/us-house-senate-members-data-leaked-for-sale>.
- Bellanova, Rocco, Kristina Irion, Katja Lindskov Jacobsen, Francesco Ragazzi, Rune Saugmann, and Lucy Suchman. 'Toward a Critique of Algorithmic Violence'. *International Political Sociology* 15, no. 1 (1 March 2021): 121–50. <https://doi.org/10.1093/ips/olab003>.
- Biswas, Soutik. 'India Election 2019: Are Fears of a Mass Hack Credible?' BBC News, 25 January 2019. <https://www.bbc.com/news/world-asia-india-46987319>.
- Brown, Ian, Christopher T Marsden, James Lee, and Michael Veale. 'Cybersecurity for Elections: A Commonwealth Guide on Best Practice'. London: The Commonwealth, 2020.
- Chandak, Anuj. 'Responsible and Ethical Use of Social Media Platforms and Strict Avoidance of Any Wrongful Use by Political Parties and Their Representatives during MCC Period in General Elections and Byelections-Regd', 6 May 2024. <https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf>.
- Chaudhary, Tarun, Thomas Chanussot, and Manuel Wally. 'Understanding Cybersecurity Throughout the Electoral Process: A Reference Document'. International Foundation for Electoral Systems, 2023. https://www.ifes.org/sites/default/files/2023-06/Understanding-Cybersecurity-Throughout-the-Electoral-Process_1.pdf.
- Coles-Kemp, Lizzie, and René Rydhof Hansen. 'Walking the Line: The Everyday Security Ties That Bind'. In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings*, edited by Theo Tryfonas, 464–80. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-58460-7_32.
- Crerar, Pippa. 'Labour Glitch Put Voting Intentions Data of Millions at Risk'. *The Guardian*, 16 April 2023. <https://www.theguardian.com/politics/2023/apr/16/labour-glitch-put-voting-intentions-data-of-millions-at-risk>.
- CrowdStrike. 'External Technical Root Cause Analysis — Channel File 291'. CrowdStrike, 6 August 2024. <https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf>.
- Davis, Barney. 'Meet AI Steve: The Bot-Driven Politician Using Artificial Intelligence on the Campaign Trail'. *Independent*, 11 June 2024. <https://www.independent.co.uk/news/uk/politics/election-politics-uk-ai-steve-brighton-b2559777.html>.
- Dutt, Barkha. 'Indian Politicians Are Bringing the Dead on the Campaign Trail, with Help from AI'. *Rest of World* (blog), 6 May 2024. <https://restofworld.org/2024/dead-relatives-ai-deepfake-india>.
- Dwyer, Andrew. 'The Recursive, Geopolitical, and Infrastructural Expertise of Malware Analysis and Detection'. In *The Practices and Politics of Cybersecurity Expertise*, edited by Rebecca Slayton and Lilly Muller, Vol. Policy Roundtable III-4. H-Diplo. H-Diplo, the Diplomatic and International History discussion network, 2024.
- Economist Intelligence. 'Democracy Index 2023: Age of Conflict'. Economist Intelligence Unit, 2024.
- Edelman, Adam. 'States Turn Their Attention to Regulating AI and Deepfakes as 2024 Kicks Off'. *NBC News*, 22 January 2024. <https://www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122>.
- Edwards, Benj. 'Due to AI Fakes, the "Deep Doubt" Era Is Here'. *Arstechnica*, 19 September 2024. <https://arstechnica.com/information-technology/2024/09/du-to-ai-fakes-the-deep-doubt-era-is-here/>.
- Financial Express. 'The Upsides, the Downsides, and the Risks of Artificial Intelligence in Elections'. *Financial Express*, 20 May 2024. <https://www.financialexpress.com/opinion/the-upside-the-downside-and-the-risks-of-artificial-intelligence-in-elections/3494892>.
- Fistsilis, Fotios, Jörn von Lucke, and Franklin De Vrieze. 'Guidelines for AI in Parliaments'. Westminster Foundation for Democracy (WFD), July 2024. <https://www.wfd.org/sites/default/files/2024-07/wfd-ai-guidelines-for-parliaments-2024-english.pdf>.
- Frankovic, Kathy. 'Russia's Impact on the Election Seen through Partisan Eyes'. *YouGov*, 9 March 2018. <https://today.yougov.com/politics/articles/20383-russias-impact-election-seen-through-partisan-eyes>.
- Garnett, Holly Ann, and Toby S. James. 'Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity'. *Election Law Journal: Rules, Politics, and Policy* 19, no. 2 (1 June 2020): 111–26. <https://doi.org/10.1089/elj.2020.0633>.

REFERENCES

- Grobelnik, Marko, Karine Perset, and Stuart Russell. 'What Is AI? Can You Make a Clear Distinction between AI and Non-AI Systems?' OECD. OECD.AI Policy Observatory, 6 March 2024. <https://oecd.ai/en/wonk/definition>.
- Harding, Luke. 'Top Democrat's Emails Hacked by Russia after Aide Made Typo, Investigation Finds'. *The Guardian*, 14 December 2016. <https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds>.
- Heibert, Kyle. 'Generative AI Risks Further Atomizing Democratic Societies'. *Centre for International Governance Innovation* (blog), 26 February 2024. <https://www.cigionline.org/articles/generative-ai-risks-further-atomizing-democratic-societies>.
- Heikkilä, Melissa. 'What the US Can Learn from the Role of AI in Other Elections'. *MIT Technology Review*, 24 September 2024. <https://www.technologyreview.com/2024/09/24/1104347/what-the-us-can-learn-from-the-role-of-ai-in-other-elections>.
- Janjeva, Ardi, Anna Gausen, Sarah Mercer, and Tvesha Sippy. 'Evaluating Malicious Generative AI Capabilities: Understanding Inflection Points in Risk'. Centre for Emerging Technology and Security. The Alan Turing Institute, n.d. https://cetas.turing.ac.uk/sites/default/files/2024-07/cetas_briefing_paper_-_evaluating_malicious_generative_ai_capabilities.pdf.
- Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions'. *Information Fusion* 97 (1 September 2023): 101804. <https://doi.org/10.1016/j.inffus.2023.101804>.
- Manheim, Karl, and Lyric Kaplan. 'Artificial Intelligence: Risks to Privacy and Democracy'. *Yale Journal of Law & Technology* 21 (2019): 106–88.
- Manning, Christopher. 'Artificial Intelligence Definitions', September 2020. <https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf>.
- Martin, Ciaran. 'Deepfakes Are Here and Can Be Dangerous, but Ignore the Alarmists—They Won't Harm Our Elections'. *The Guardian*, 11 June 2024, sec. Opinion. <https://www.theguardian.com/commentisfree/article/2024/jun/11/deepfakes-ignore-alarmists-elections>.
- McLean, Scott, Gemma J. M. Read, Jason Thompson, Chris Baber, Neville A. Stanton, and Paul M. Salmon. 'The Risks Associated with Artificial General Intelligence: A Systematic Review'. *Journal of Experimental & Theoretical Artificial Intelligence* 35, no. 5 (4 July 2023): 649–63. <https://doi.org/10.1080/0952813X.2021.1964003>.
- Mulligan, Scott J. 'There Are More than 120 AI Bills in Congress Right Now', 18 September 2024. <https://www.technologyreview.com/2024/09/18/1104015/here-are-all-the-ai-bills-in-congress-right-now/>
- National Institution for Transforming India. 'National Strategy for Artificial Intelligence'. National Institution for Transforming India (NITI Aayog), June 2018. <https://www.niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>.
- NCSC Assessment. 'The Near-Term Impact of AI on the Cyber Threat'. National Cyber Security Centre, 24 January 2024. <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>.
- Nimmo, Ben, and Michael Flossman. 'Influence and Cyber Operations: An Update'. OpenAI, October 2024. https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.
- Nisos. 'What India's Elections Can Teach Us About AI'. Nisos, June 2024. <https://6068438.fs1.hubspotusercontent-na1.net/hubfs/6068438/indian-elections-ai-usage.pdf>.
- NIST. 'Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile'. NIST Trustworthy and Responsible AI. National Institute of Standards and Technology, July 2024. <https://doi.org/10.6028/NIST.AI.600-1>.
- Office of Congressional and Public Affairs. 'Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers'. Bureau of Industry & Security, 20 June 2024. <https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers>.
- Office of Public Affairs. 'Three IRGC Cyber Actors Indicted for "Hack-and-Leak" Operation Designed to Influence the 2024 U.S. Presidential Election'. U.S. Department of Justice, 27 September 2024. <https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us>.
- Office of the Director of National Intelligence. 'Assessing Russian Activities and Intentions in Recent US Elections'. Intelligence Community Assessment. US Government, 6 January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
- OpenAI. 'Introducing ChatGPT'. OpenAI, 30 November 2022. <https://openai.com/index/chatgpt>.
- Orey, Rachel. 'A Proposal for Bipartisan Federal Election Reform'. Bipartisan Policy Center, 31 July 2023. <https://bipartisanpolicy.org/explainer/a-proposal-for-bipartisan-federal-election-reform>.
- Padmanabhan, Deepak, Stanley Simoes, and Muir MacCarthaigh. 'AI and Core Electoral Processes: Mapping the Horizons'. *AI Magazine* 44, no. 3 (1 September 2023): 218–39. <https://doi.org/10.1002/aaai.12105>.
- Pasricha, Anjana. 'AI, Deepfakes, Social Media Influencers—India's Mammoth Election Sees It All'. VOA, 22 May 2024, sec. South & Central Asia. <https://www.voanews.com/a/ai-deepfakes-social-media-influencers---india-s-mammoth-election-sees-it-all-/7622336.html>.

REFERENCES

- Radu, Roxana. 'The G20 and Global AI Governance'. AI4Democracy. IE University, July 2024. https://static.ie.edu/CGC/G20_Global_AI_Governance.pdf.
- . 'The Variable Geometry of AI Governance', 5 February 2024. <https://www.genevapolicyoutlook.ch/the-variable-geometry-of-ai-governance/>.
- Ramaciotti, Pedro. 'Depolarizing and Moderating Social Media with AI'. AI4Democracy. Centre for the Governance of Change, IE University, July 2024. <https://static.ie.edu/CGC/AI4D%20Paper%20%20Depolarizing%20and%20Moderating%20Social%20Media%20with%20AI.pdf>.
- Rebello, Karen. 'India's Generative Ai Election Pilot Shows Artificial Intelligence in Campaigns Is Here to Stay'. Series on Generative Artificial Intelligence and Elections. Center for Media Engagement, October 2024. <https://mediaengagement.org/wp-content/uploads/2024/10/Indias-Generative-AI-Election-Pilot-Shows-Artificial-Intelligence-In-Campaigns-Is-Here-To-Stay.pdf>.
- Rest of World. 'Maduro Pledges to Cede Power in Faked Video', 28 July 2024. <https://restofworld.org/2024/elections-ai-tracker/#/maduro-false-concession-pledge-venezuela>.
- Robins-Early, Nick. 'Trump Posts Deepfakes of Swift, Harris and Musk in Effort to Shore up Support'. *The Guardian*, 19 August 2024. <https://www.theguardian.com/us-news/article/2024/aug/19/trump-ai-swift-harris-musk-deepfake-images>.
- Sampathkumar, Mythili. 'US Cyber Security Official Says 21 States' Voter Rolls Were Hacked during 2016 Election'. *Independent*, 8 February 2018. <https://www.independent.co.uk/news/us-election-hacking-voter-rolls-states-us-cyber-security-russia-hackers-crime-trump-a8201041.html>.
- Shukla, Vandinika, and Bruce Schneier. 'Indian Election Was Awash in Deepfakes—but AI Was a Net Positive for Democracy'. *The Conversation*, 10 June 2024. <https://theconversation.com/indian-election-was-awash-in-deepfakes-but-ai-was-a-net-positive-for-democracy-231795>.
- Simon, Felix M., Keegan McBride, and Sacha Altay. 'AI's Impact on Elections Is Being Overblown'. *MIT Technology Review*, 3 September 2024. <https://www.technologyreview.com/2024/09/03/1103464/ai-impact-elections-overblown>.
- Stockwell, Sam. 'AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections'. Centre for Emerging Technology and Security. The Alan Turing Institute, September 2024. https://cetas.turing.ac.uk/sites/default/files/2024-09/cetas_briefing_paper_-_ai-enabled_influence_operations_-_threat_analysis_of_the_2024_uk_and_european_elections.pdf.
- Summers, Evan, Sarah Moulton, and Chris Doten. 'Cybersecurity Handbook for Parliaments'. National Democratic Institute (NDI) and House Democracy Partnership, 2022. https://www.ndi.org/sites/default/files/%5BEN%5D%20Cybersecurity%20Handbook_Parliaments.pdf.
- Tashman, Alexandra. "'Malicious Deepfakes"—How California's A.B. 730 Tries (and Fails) to Address the Internet's Burgeoning Political Crisis'. *Loyola of Los Angeles Law Review* 54, no. 4 (2021): 1391–1422.
- Texas. An act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election., S.B. No. 751 § (2019). <https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm>.
- The Electoral Commission. 'Information about the Cyber-Attack', 30 July 2024. <https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems/information-about-cyber-attack>.
- Thornhill, John. 'Deepfakes Pose a Particular Threat, but They Are Not as Dangerous as You Think'. *The Irish Times*, 27 June 2024. <https://www.irishtimes.com/business/2024/06/27/deepfakes-pose-a-particular-threat-but-they-are-not-as-dangerous-as-you-think>.
- UK Government. 'Ministerial Taskforce Meets to Tackle State Threats to UK Democracy', 28 November 2022. <https://www.gov.uk/government/news/ministerial-taskforce-meets-to-tackle-state-threats-to-uk-democracy>.
- . 'UK Holds China State-Affiliated Organisations and Individuals Responsible for Malicious Cyber Activity', 2 April 2024. <https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity>.
- Vassilev, Apostol, Alina Oprea, Alie Fordyce, and Hyrum Anderson. 'Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations'. NIST Trustworthy and Responsible AI. NIST Artificial Intelligence (AI) Report. NIST, January 2024. <https://doi.org/10.6028/NIST.AI.100-2e2023>.
- Whyte, Christopher. 'Cyber Conflict or Democracy "Hacked"? How Cyber Operations Enhance Information Warfare'. *Journal of Cybersecurity* 6, no. 1 (1 January 2020): tyaa013. <https://doi.org/10.1093/cybsec/tyaa013>.
- Wilde, Gavin. 'The Misguided Emphasis on U.S. Political Campaign Hacks'. Carnegie Endowment for International Peace. *Emissary* (blog), 27 August 2024. <https://carnegieendowment.org/emissary/2024/08/iran-trump-campaign-hack-election-security?lang=en>.
- World Bank Group. 'GDP per Capita (Current US\$)', 23 September 2024. <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD>.

Written by:

Andrew C. Dwyer
Roxana Radu

This paper is part of a series of four papers within AI4Democracy, a global research and outreach initiative led by the Center for the Governance of Change at IE University, with Microsoft as strategic supporter. AI4Democracy seeks to harness AI to defend and strengthen democracy through coalition-building, advocacy, and intellectual leadership.

Suggested citation:

Dwyer, A., Radu, R. (2024). *Enabling Secure Democratic Ecosystems through AI*, AI4Democracy, IE Center for the Governance of Change.

© 2024, CGC Madrid, Spain

All Images were generated by different AI tools.

Design: epqstudio.com

**FOR MORE INFORMATION ON THE
AI4DEMOCRACY INITIATIVE, VISIT:**

[IE.EDU/CGC/RESEARCH/AI4DEMOCRACY](https://ie.edu/cgc/research/ai4democracy)



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License. To view a copy of the license, visit creativecommons.org/licenses/by-nc-sa/4.0