



Funded by
the European Union



SELECT

Sustaining Peace During
Electoral Processes project

PEACEFUL AND INCLUSIVE ELECTIONS IN A DIGITAL AGE

Based on challenges shared and
programmatic options identified
during the SELECT research and
the Global Conference organized
8, 9, 10 November 2023



The views expressed in this publication are those expressed during the 2.5 days conference and do not necessarily represent the views of the United Nations Development Programme (UNDP), or any Member States. Moreover, the contents of this publication shall not be taken to reflect the views of the European Commission.

Copyright © UNDP 2024. All rights reserved.

Preferred citation: UNDP (2023). SELECT Conference Report: Peaceful and Inclusive Elections in digital Age.

United Nations Development Programme

One United Nations Plaza.

New York, NY 10017 USA

ACKNOWLEDGMENTS

This report has been drafted by:

Gianpiero Catozzi

Ajay Patel

Lucas Fernandez-Corredor

Saré Knoope

Graphic designer:

Adelaida Contreras

Photos:

Dafne Morcillo

**SELECT**

Sustaining Peace During
Electoral Processes project

PEACEFUL AND INCLUSIVE ELECTIONS IN A DIGITAL AGE

Based on challenges shared and
programmatic options identified
during the SELECT research and
the Global Conference organized
8, 9, 10 November 2023



TABLE OF CONTENTS

6	●	Executive Summary
7		Democratic governance in the digital age
7		Digital threats to elections
8		How to protect the electoral information environment
9		Detect and response to information pollution
9		Building public resilience to information pollution
9		Approaches to regulating political speech and information pollution
10		Digital Inclusion, and exclusion
10		Violence against women
10		Youth participation in the digital elections
11		Election administration in the digital age
12	●	Introduction
15	●	Democratic governance in the digital age
17	●	Information integrity and the challenge to elections across the world
22	●	Artificial intelligence and the electoral information ecosystem
25	●	Dynamics of election-related violence
27	●	Protecting the election information ecosystem
30	●	Identifying and responding to information pollution
33	●	Building public resilience to information pollution
36	●	Approaches to regulating political speech and information pollution
39	●	Inclusion within the Electoral Process
41		Advancing inclusion in the Digital Era
42		Digital exclusion
45	●	Online and offline violence against women in public life
48	●	Youth participation for peaceful and inclusive electoral process
50	●	UNDP Digital Tools for Information Integrity
52	●	Future elections: how technology and innovations will shape elections over the next decade
52		An unclear but forward technological roadmap
54		Trust and technology in elections
55		Exposure to cyber attacks
56		Definition Box: Cybersecurity
57		The enduring digital divide
59		Artificial intelligence within election administration
63	●	SELECT Agenda and Speakers



EXECUTIVE SUMMARY

How to achieve credible, inclusive and peaceful elections in the digital age, whilst benefiting from the advantages of modern technology? This question is set to define how elections evolve over the coming years and decades.

An election can be evaluated on several axes, but perhaps one of the fundamental measures is the degree of confidence various stakeholders have in the process. It is a leading factor in the ultimate acceptance of the results and the potential for electoral or political violence. Much investment has been made in exploring how to build confidence in elections, such as professional election delivery, inclusive processes, independent bodies, transparency, amongst others.

The digital age has introduced new dynamics to the relationship between stakeholders and their confidence in electoral processes. The main waves of disruption are tectonic changes in how people communicate, and new technological solutions to public service delivery. For some,

these developments may support more successful elections and vibrant democracies. Other fear these may fatally undermine public confidence in elections and democratic institutions.

Technologies potential is inherently contradictory. It can be simultaneously divisive and unifying. Exclusive and inclusive. Which outcomes prevail are a function of how they are designed, deployed, the context in which they are deployed and the actions of electoral stakeholders.

To gain an insight on how to achieve favoured electoral outcomes, the European Union Foreign Policy Instrument and UNDP held a Global Conference in Brussels from 8-10 November 2023, under the Sustaining Peace during Electoral Processes "SELECT" Project conference. The event allowed the engagement of election practitioners and information integrity experts from around the world to exchange view and experiences, pose recommendations, and identify questions.

Below are key takeaways from this event and the work of UNDP, providing considerations for engaging with elections in the digital age:

Democratic governance in the digital age

1. **Democracy has been in regression for years.** Disruption in the modes and ownership of political communication invoked by technology has been posited by many as contributing to this decline.
2. Digital technologies hold the potential to contribute towards societal good and ill. The ultimate impact of technology upon democratic governance rests upon a number of factors, including the design of the technology itself, prioritisation of trust and safety, governance frameworks, and socio-political-technological context within which they are deployed. It is vital that **local and global efforts** strive to establish conditions which support technology to contribute towards human flourishing, including through international regulatory means.
3. Despite the need for more international cooperation in the digital age, **a lack of consensus over fundamental norms** makes it difficult to determine how empowering or corrosive technology is, or often what is classified as a societal good. While challenging, enhancing global conversations on this is essential to future democratic governance.
4. **Service delivery** is fundamental to good governance, and technology has the potential to reform practice, with inclusion and effectiveness at its core.

Digital threats to elections

5. Within this document, are a **myriad of ways the digital age has reinforced or introduced new dynamics to electoral processes**. These phenomena are inextricably intertwined, calling for a holistic consideration of digital threats to elections, and how they can be averted. Looking forward, threats will inevitably grow as practice innovates and technologies emerge, not least artificial intelligence.
6. There are a range of **digital threats to elections**, and while information pollution is a considerable one, it is not alone. Other examples include; censorship, internet shutdowns and throttling, cybersurveillance, privacy violations and cyberattacks.
7. There is a broad consensus between election practitioners, information integrity practitioners and the general public that **information pollution is a material concern to elections across the world**, with many countries already believing it to have had a deleterious impact upon their elections. They also agree there are insufficient protections in place to challenge its impact.
8. Online information pollution has offline and historical analogies, and their potency is frequently **rooted in broader grievances**.
9. However, the **internet**, and particular social media platforms, have a set of features which can **amplify information pollution** in ways beyond **legacy media and traditional information distribution methods**.
10. The **election period introduces additional characteristics** which further complicate the information ecosystem. The spike in political activity, the broad and partisan public stakes, international interests, high stakes to candidates and votes alike, a requirement for plurality and inclusion of political speech, and the need to provide a level playing field, are just some of the features.
11. The election also introduces a number of specific **targets** for information pollution campaigns, including the **election management body**, and the election process itself. Credible elections have always relied upon the perceived legitimacy of the administrative institution and its work, which can be unduly undermined by information pollution.
12. Political actors have long deployed **electoral violence** to advance their electoral interests, often using disinformation as a tactic to mobilise their supporters, undermine their opponents, or promote false narratives about the electoral process. There are concerns that the internet, and online platforms, have provided an under regulated yet potentially powerful medium to instigate electoral violence with few, if any, consequences. There is also a fear that major platforms are designed with the goal of maximising user engagement. This includes elevating content designed to trigger emotional responses, which in turn potentially contributes to electoral violence.

13. **Artificial Intelligence** is preoccupying the electoral and disinformation communities, as it is many other fields. Artificial Intelligence is expected to have a transformative influence upon much of modern life, and elections are not exempted. Generative AI will make the production of seemingly authentic and evocative harmful content easier, cheaper and more scalable. AI may also be deployed to support the distribution of information pollution, including through the creation of fake accounts or facsimileing convincing engagement.
14. **Building protections against the weaponization of Artificial Intelligence** in electoral information environments is vital but complex, with defenses likely to incorporate regulatory, educational and technological approaches. There is a need for international cooperation given the global nature of the issue.
15. **Artificial intelligence** also promises to support the integrity and inclusion of elections, both as a counter measure to adversarial AIs, but it may also hold **create new opportunities** for greater participation, voter information and equal competition.

How to protect the electoral information environment

16. The digital age poses numerous and significant challenges to the electoral information environment, demanding **a new family of activities** designed to promote information integrity and protect the election process.
17. The electoral authorities, other governmental bodies, civil society, platforms, academic, the media and the political contestants are the **key actors involved in the electoral information space**. Each holds the potential to strengthen or weaken the information environment, through their actions, or inaction. The role each actor has to play is guided by the various contextual factors, such as mandates, capacities and the political dynamics.
18. EMBs and the processes they oversee may be victim to information pollution. To be better able to respond to such concerns, EMBs with capacities to identify and counter information pollution, and communicate timely and accurate information to the public may be better able to support credible elections.
19. Because of the complex nature of the challenge, effective responses to information pollution require a holistic and systemic approach with a diverse set of actors holding different strengths and constituencies. A recommended approach for actors in this space is **multi-stakeholder engagement**, establishing structures which allow them to work in concert and to be coherent and coordinated in the various activities related to promoting information integrity. These mechanisms may come in the form of coordination bodies, loose information sharing groups, communities of practice, or more formal arrangements to collaborate on specific activities including agreed interpretation of data, the prioritization of issues and organising collective responses to name a few. Furthermore, such engagement will permit the sharing of knowledge, and a greater capacity of advocacy. For example, EMBs may not always be best placed to address certain narratives about the elections and partnerships with fact-checking organizations could address any potential conflict of interest and/or capacity challenge EMBs may face.
20. Where possible, the responses should be guided by a **strategy** – a strategy which may complement a broader national vision of how to tackle the challenges of information pollution. These may be plans for the governmental institutions, or a broader multi-stakeholder vision, depending upon the realities of the context. Strategies are expected to be inline with international human rights law, and designed around the country situation.
21. While there is a spike in information pollution during the operational and campaigning period directly preceding an election, a more **longitudinal vision** is important to address increasingly protracted attacks on electoral institutions that are pre-emptive as well as well financed, informed and organised, and strengthening broader resilience in advance of the peaks, which takes time to establish
22. When conceptualising a program of activities, a **framework** can be developed on 1) how to **detect and respond** to information pollution during the election 2) how to build the underlying **public resilience** to information pollution, 3) how to **regulate** the landscape to deter actors from disseminating information pollution and platforms for facilitating it. More detail on each can be found on the SELECT website [Information Integrity Report – Select \(sustainingpeace-select.org\)](https://sustainingpeace-select.org)

Detect and response to information pollution

23. Identifying and responding to information pollution in the course of an election process is a critical area of work when attempting to defend an on-going election. Approaches such as **online content monitoring and analysis, fact checking, open source investigations and strategic communication** are common.
24. There may be various actors charged with defending the electoral information environment. Part of this responsibility is to monitor the information environment and effectively address harmful content and narratives. However, there is a broad consensus that **content level responses are not sufficient**.
25. Fact checking, as an activity typically delivered by civil society, media and other civilian groupings, is a vital and popular activity around election processes. However, its limitations in reaching and affecting the views shaped by information pollution need to be acknowledged. In turn, these limits inform which complementary actions are selected, designed and delivered.
26. Election management bodies are well advised to invest in tools and structures including partnerships to better understand and respond to the information environment, as well as develop their strategic communications competences to better defend their staff, the institution, and the election process from malicious actors.

Building public resilience to information pollution

27. Efforts to build greater personal resilience to information pollution can focus on **building public digital skills and education**. This stream of work can mitigate weaknesses in content related approaches.
28. **Civic education** has been a long-standing activity within the election process. Spreading accurate and engaging information can pre-empt attempts to spread misleading or harmful narratives. However, this field should be expanded to build voter awareness of and resilience to potential information pollution campaigns.
29. Enhancing **digital literacy and critical thinking** are vital to building broad public resilience to modern information pollution. It is an area of work only recently gaining popularity, yet its impact is still being ascertained. Ensuring rigorous accompanying research and evaluation is important to allow the community to understand what works.
30. Building an **information ecosystem which provides reliable and trusted information** is vital and can be approached by various means. Closing the news/information gaps can be attempted by supporting independent local and community media, promoting journalistic capacities and building public interest media. The election management body, civil society, and the media can all contribute to this effort. Depending upon the country dynamics and the activity under discussion, different actors may be better placed than others. EMBs in particular are encouraged to adapt to the new information reality, build teams, budget for disinformation resources and capacities, etc.

Approaches to regulating political speech and information pollution

31. **Influencing the behaviour of political actors in the information environment** can provide another approach to constrain and disincentivize the propagation of information pollution. There are a range of approaches, such as legally binding to voluntary guidelines, and from supranational frameworks to extremely local agreements. Fundamentally, coercing political actors, platforms and media to contribute to the healthy information ecosystem – either through legal or political means – can be beneficial if successful.
32. Any approach to create accountability within the electoral information ecosystem should **prioritise human rights approaches**, most relevant of which is freedom of expression.

- 33. A multi-stakeholder approach is warranted during the design of any regulatory activity. It is the right of **vulnerable groups and communities to be included** in the conversations taking place – be in at a local, national or international level.
- 34. **Regulation of online platforms** can be used to shape the information environment towards promoting reliable information, reducing information pollution and assigning accountability to what has become a set of key actors in the election process. A word of caution is required, however, as regulatory processes are open to abuse and manipulation.
- 35. Codes of Conduct can provide a more agile means of building guard-rails around the **activities of political parties and other electoral actors** and provide a means to avoid some of the concerns around government abuse. However, these approaches must be designed in a context specific manner in order to be effective, including consideration towards monitoring and enforcement.

Digital Inclusion, and exclusion

- 36. **Inclusion is a fundamental tenant** in the conduct of elections, however, despite various efforts some contexts have experienced a regression in recent years.
- 37. **Democratic participation can flourish** as a result of digital technology, allowing for increased means for participation and community engagement, new ways to access information and the provision of accessible election technology. Data can improve programming and services delivery.
- 38. However, some of the **observed decline in inclusion** is likely to be a result of technology in the political sphere, with factors such as the digital divide, lack of trust, and systematic bias undermining inclusion.
- 39. As technology is introduced within elections, stakeholders should **consider its impact upon inclusion**, paying attention to intersectionality, and designing methods to alleviate inequities – for election administration but also within the information environment.

Violence against women

- 40. Online violence against women has become an **endemic concern within elections**, deployed to make public life untenable for aspiring female politicians and supporters.
- 41. The issues of gendered online discrimination are **underpinned by more fundamental prejudices** within societies – biases held be both women and men. Accordingly, programmatic options should acknowledge and address these underlying drivers.
- 42. Despite the disturbing extent of abuse against women, there are **a range of activities that can and should be deployed** to protect them, strengthen their participation and introduce accountability ranging from awareness raising and engagement to capacity building and legislative reform coupled with enforcement strategies.

Youth participation in the digital elections

- 43. It is crucial to involve youth in the **design and execution of activities** intended to promote peaceful and inclusive elections, in order to increase their potential for success.
- 44. Despite the value of using technology to engage youth within the electoral process, it **can be inadequate** to meaningfully engage in all circumstances – especially where there is intersectionality with other attitudinal or material constraints.

Election administration in the digital age

45. **Digital transformation of election administration** has been a prominent concern for election management bodies for many years, with many undertakings important reforms to make services more accessible, efficient and secure. It is an area in which a number of participants to the Global Conference reported their need for greater assistance.
46. Successful digital transformation in the context of electoral administration requires approaches which **prioritise the building of public trust** in the technology and the broader electoral process.
47. Key ways of building confidence around the deployment of electoral technology include a **gradual roll out** that allows trust to be established in a measured fashion. Also vital is a professional election administration capable of taking all measures possible to deliver a **successful deployment**, even if the scale of the initial rollouts is limited.
48. Considerations about **accessibility and the digital divide** are expected to remain relevant for the foreseeable future. They should remain front of mind when devising new technologies intended to reach voters, or other stakeholders.
49. **Cyber-security** is an acute concern for election administrators as they face increasingly sophisticated and varied threat actors. Building appropriate structures, engaging specialists and building strong digital capacities can provide a significant improvement in the integrity of the election management bodies digital infrastructure.
50. **Artificial intelligence is of rising interest** to the community of election administrators, with hopes that it can provide important benefits to how elections are delivered. Already there is adoption of AI tools by electoral authorities seeking to enhance their work. Its application is envisaged in various aspects of their work, potentially enhancing current approaches, or even transforming the nature of election administration.
51. Artificial Intelligence within the sensitive area of election delivery should be approached with **due diligence**. Despite its potential contributions, it is still in its nascently, especially within the context of election administration. With this emerging practice comes a non-negligible risk, of either failure or, worse still, unintended, and deleterious outcomes.

The digital age is changing how to deliver credible elections. Election practitioners across the world are navigating this new world, with both optimism and trepidation. There is no denying that in many ways, the next generation of elections will differ vastly from those that have come before. Throughout the various stages of the SELECT project, various examples of innovative practices in electoral inclusion and integrity have been shared. And yet, the new hurdles reassert the importance of enduring electoral principles for electoral administration.

More than ever, **professional** election administration is needed to tackle potentially highly technical operations and complex threats. In an information environment where a small infraction can be leapt on with accusations of obscene bias, maintaining actual and perceived **independence and impartiality** of election management administration has never been more important, or difficult. **Transparency** is of even greater importance, with information vacuums more easily filled by malicious actors.

In practice, these principles can hold contradictions and require difficult decisions, especially in line with some of the recommendations discussed. For example: as electoral digital infrastructure is intertwined with various private and public institutions, dependences increase, and some degree of **independence of action** will be traded for efficiencies. Building all-of-society responses to information threats have been highlighted as vital but can invite accusations of **impartiality**. **Professionalism** is inescapable, but it also a matter of degree – which needs to be weighed against costs. **Transparency** is important, but with adoption of the complex algorithms, will be harder to be meaningfully understood. Evaluating trade-offs is no simple feat. The technical complexities make it harder to reach informed decisions.

The collective design and adoption of standards and best practice in these areas becomes particularly important. Looking forward, UNDP strives to support the electoral community in exploring these necessary questions.



INTRODUCTION

How to achieve credible, inclusive and peaceful elections in the digital age, whilst benefiting from the advantages modern technology bring? This fundamental question is set to define how elections evolve over the coming years and decades.

An election can be evaluated on several axes, but perhaps the fundamental measure is the degree of confidence various stakeholders have in the process. It is a leading factor in the ultimate acceptance of the results and the potential for electoral or political violence. Much investment has been made in exploring how to build confidence in the election, such as professional election delivery, inclusive processes, independent bodies, transparency, amongst others.

The digital age has introduced new dynamics to the relationship between stakeholders and their confidence in elections. The main waves of disruption are tectonic changes in how people communicate, and new technological solutions

to public service delivery. Some fear these may fatally undermine public confidence in elections and democratic institutions. Alternatively, others believe these new technologies may support more successful elections and vibrant democracies.

Technology is inherently contradictory. It can be simultaneously divisive and unifying. Exclusive and inclusive. Which outcomes prevail are a function of how they are designed, deployed, the broader environment and the actions of electoral stakeholders.

To gain an insight on how to achieve favoured electoral outcomes, the European Union Foreign Policy Instrument and UNDP held a Global Conference in Brussels from 8-10 November 2023, under the Sustaining Peace during Electoral Processes "SELECT" Project conference. The event allowed the engagement of election practitioners and information integrity experts from around the world to exchange view and experiences, pose recommendations, and identify questions.

The digital age is changing how to deliver credible elections. Election practitioners across the world are navigating this new world, with both optimism and trepidation.

And yet, the new hurdles reassert the importance of enduring electoral principles for electoral administration.

More than ever, professional election administration is needed to tackle potentially highly technical operations and complex threats. In an information environment where a small infraction can be leapt on with accusations of obscene bias, maintaining actual and perceived independence and impartiality of election management administration has never been more important, or difficult. Transparency is of even greater importance, with information vacuums more easily filled by malicious actors.

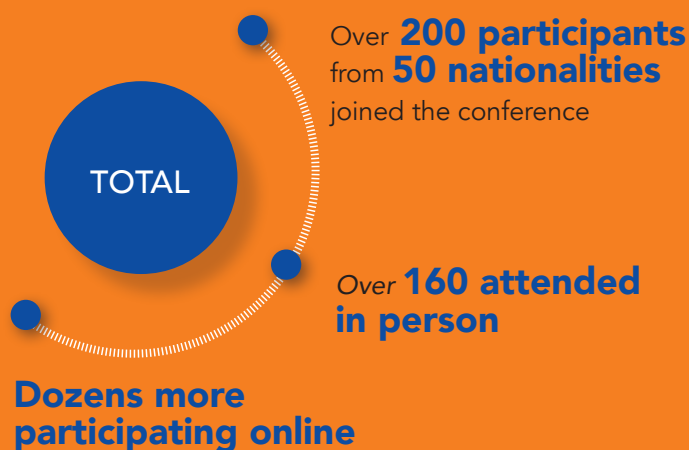
In practice, these principles can hold contradictions and require difficult decisions, especially in line with some of the recommendations discussed. For example: as electoral digital infrastructure is intertwined with various private and public institutions, dependences increase, and some degree of independence of action will be traded for efficiencies. Building all-of-society responses to information threats have been highlighted as vital, but can invite accusations of impartiality. Professionalism is inescapable, but it also a matter of degree – which needs to be weighed against costs. Transparency is important, but with adoption of the complex algorithms, will be harder to be meaningfully understood. Evaluating trade-offs is no simple feat. The technical complexities make it harder to reach informed decisions.

The collective design and adoption of standards and best practice in these areas becomes particularly important. Looking forward, UNDP strives to support the electoral community in exploring these necessary questions.

CONFERENCE DETAILS:

The overall goal of the conference was to reflect on the complexities and opportunities presented to electoral actors by the digital age as they work towards peaceful and inclusive elections. To this end, the conference brought together practitioners, to exchange best practices, identify gaps, and bolster partnerships and expertise.

The report reflect the discussions held and the opinions, research and insights shared by the various panellists and participants over the course of the 2,5 day conference.



SELECT PROJECT:

SELECT is a research project and programming tool in one, with programming strategies and activities made publicly available to practitioners on a dedicated Knowledge Hub; informed by an inclusive and consultative research process that identifies the challenges and actionable solutions in relation to the elections-conflict prevention nexus. SELECT focuses on various topics considered relevant to the likelihood of electoral violence, including information integrity, women's participation and youth participation.

SELECT is the fruit of an initial research phase which concluded that current programming around elections would benefit from a reinforced preventive perspective and long-term activities to address election-related violence.

Furthermore, SELECT builds on the acknowledgement that there is a need to bring together the various communities of practice while embedding electoral support in broader governance work.



Against this background, the overall objective of the “*Sustaining Peace during Electoral Process*” (SELECT) project is to build the capacity of both national electoral stakeholders and international partners to:

identify risks factors that may affect elections; design

programmes and activities specifically aimed at preventing and reducing the risk of violence; and

implement operations related to the electoral processes in a conflict sensitive manner.

SELECT PROJECT:

The conference was structured around **10 substantive sessions**, using various formats designed to draw out key points and audience participation.

Democratic governance in the digital age

Information pollution dynamics and other digital threats

Approaches to strengthen the information ecosystem


Dynamics of election related violence

Electoral inclusion within the electoral process

Violence against women in public life – online and offline

Election administration within the digital age

UNDP's information integrity programming and tools



DEMOCRATIC GOVERNANCE IN THE DIGITAL AGE

Human rights and the rule of law have been in recession for several years, with an accompanying increase in contested elections, unconstitutional changes of government and a decline in trust in formal political systems. Low levels of public engagement with political systems reflect a lack of inclusion.

The role of technology in driving this malaise is a matter of concern. There exists a general agreement that technology is a double-edged sword when it comes to democratic advancement. Simultaneously holding the capacity to empower citizens and expand freedom of expression, yet also a medium to distribute harmful content and enhance the capacity of authorities to repress dissent and opposition. Technology has exposed elections to interference, hate speech and polarisation, and has been employed as a tool to entrench incumbents.

Once we recognise that technologies influence may be positive or negative, inevitable questions are, on balance, is the current iteration of the digital environment beneficial or harmful, and how to nurture the positives aspects.

Prior to assessing if technology is a force for democratic advancement or retreat, a normative expectation about technology is required. Determining what is virtuous is often contested, as is the fundamental nature of technology. Some view technology as a neutral tool, whose virtue or lack thereof is derived by those who wield it. Other consider it to have intrinsic value, which is in part a function of decisions made as it was built. Both are wedding to the context within which they are designed and deployed, and the objectives and underlying beliefs of the authorities and communities within a jurisdiction.

Technology has become ubiquitous. With over four billion connected individuals living in different countries and communities, developing a shared understanding of technology is extremely challenging. The variety of views on privacy and freedom of expression, two cornerstones in defining human interaction with technology, demonstrate the complexity with establishing communal norms.

This difficulty in reaching communal norms is one factor which has constrained international action, contributing to governments exploring their own technology governance approaches. There are other constraints upon multistakeholder dialogue on technology governance, such as a lack of support, funding and vested interests.

And yet, developing international frameworks around elections in a digital age is an essential task. While social media largely evaded regulation until recently, this experience has made the international community alive to the possible dangers of modern technology. Looking forward, potentially more powerful technologies will demand effective and globally agreed upon frameworks if they are to support human potential.

Technology's role in the building stronger and more inclusive democratic governance has various facets. While it is important people perceive their government as effective, it is also vital that governments actually deliver upon actual needs. Technology, of course, plays an increasingly important role in public sector delivery. Digital transformation and public digital infrastructure are becoming core to this new generation of service delivery, including elections.

The effectiveness of governance systems underpin the public perception their state and the broader democracies overseeing them. Part of improving governance and confidence in institutions is building a better understanding of how they deliver to local populations, and then putting this knowledge into action. However, public sentiment is formed by various forces, some based on personal experience and others on signals received through the information ecosystem. Building a greater insight into the deeper psychological dynamics that form individuals' opinions is valuable. As is understanding what spurs people into posting information pollution, hate speech and deploying violence online.

KEY TAKEAWAYS

- **Democracy has been in regression** for years. Disruption in the modes and ownership of political communication invoked by technology has been posited by many as contributing to this decline.
- Digital technologies hold the potential to contribute towards societal good and ill. The ultimate impact of technology upon democratic governance rests upon a number of factors, including the design of the technology itself, prioritisation of trust and safety, governance frameworks, and socio-political-technological context within which they are deployed. It is vital that **local and global efforts** strive to establish conditions which support technology to contribute towards human flourishing, including through international regulatory means.
- Despite the need for more international cooperation in the digital age, a **lack of consensus over fundamental norms** makes it difficult to determine how empowering or corrosive technology is, or often what is classified as a societal good. While challenging, enhancing global conversations on this is essential to future democratic governance.
- **Service delivery** is fundamental to good governance, and technology has the potential to reform practice, with inclusion and effectiveness at its core.



INFORMATION INTEGRITY AND THE CHALLENGE TO ELECTIONS ACROSS THE WORLD

The digital sphere has fundamentally changed the dynamics of elections. It has amplified and sophisticated the manner in which politicians can approach elections, reach out to voters, and win elections. Similarly, it has altered the ways in which civilians find information, consume news and build communities.

With this digital age have come a spectrum of good and ills. One particular concern is that the new information environment is vulnerable to manipulation. During the context of an election, a set of political, financial or geostrategic motivations make the electoral process a flashpoint for the spread of information pollution and other digital threats.

Of the electoral experts in attendance at the 2023 global conference, there was near unanimity that information pollution was a concern for their work. Over 60% believed that information pollution had

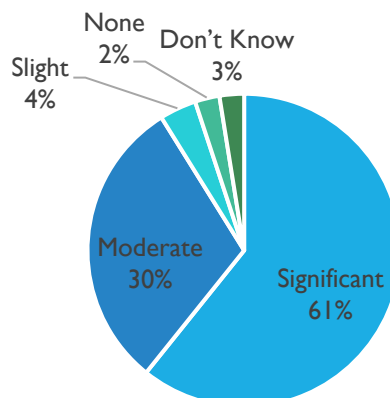
severely undermined the credibility of elections in their country, with 30% believing the impact to have been moderate.

These concerns reflect a similar sentiment amongst the general global public, with a recent global IPSOS survey finding that 85% of those questioned were worried about misinformation and disinformation, with 87% affirming that misinformation had already impacted their countries' electoral processes. The same survey indicated that a majority of respondents received their news from social media platforms, which evidently raises the stakes of information pollution and the need to tackle it.

The EU External Action Service has invested in methodical studies of media environments in the countries they monitor elections in. From this, they have found an increase in information manipulation and use of social media platforms.

FORM STATISTICS

Survey Question: How much has information pollution undermined the credibility of previous elections in your country?



To some extent, the concerns around elections and information pollution are irrespective of the digital sphere. Propaganda, political violence, or quite simply, politicians lying, have existed long before elections were even conceived. There are also modern-day offline counterparts to the online harms – disinformation is too commonly spread through and by traditional media, and many media outlets also share a financial interest in the driving viewership.

However, there are features of the digital age which warrant renewed action. The scale of information pollution that can be produced and shared on the internet can be almost infinite. The speed by which information can spread is potentially immediate. The decentralised nature of the internet allows communities to form easily and anonymously. The vast number of online groups and online news outlets confounds traditional monitoring and regulation.

While some of these concerns may be manageable outside of an election, the spike in political activity that accompanies an election can overwhelm common defences and pull people who otherwise don't pay attention to the machinations of politicians into dangerous narratives.

Furthermore, the election throws up a new target for scrutiny and assault – the electoral management bodies. Tasked with delivering the technical process of elections, they can be poorly equipped to handle a dynamic and adversarial information barrage. In this time of growing distrust towards institutions – often fuelled by the very politicians seeking electoral gain – election management bodies are dangerously placed to weather concerted attacks.

These concerns are more acute for election management bodies from the Global South. Given the essential nature of 'big tech' platforms in this debate, they have expressed a fear that without being a significant profit centre, the ability for the EMB, or country, to influence the platform is limited.

While the regulation of electoral campaigns is a normal part of any election, the digital age has transformed the paradigm. The internet has invited a host of new voices to electoral politics, often straddling the political spectrum, skirting the fringes. The intrinsically pluralistic and competitive nature of elections imposes a particularly high threshold for what speech or content should be censored. The lack of clear definitions, the absence of a common and detailed agreement on content policies and the inherent complexities of applying subjective frameworks at such a massive scale, all contribute to inherent challenges and unsatisfactory decisions.

Much of the past two decades have been defined by the spread of social media. And while growth in social media usage continues apace, in some countries they have already more or less reached their plateau. However, how users navigate social media is shifting. The number of platforms is expected to expand, each providing different features and creating new overheads for would-be creators – including election management bodies.

The idea of a common public square, a place where everyone is, is likely to be less and less the case. Instead, a more challenging possibility is one where fringe communities gather in obscure parts of the internet, where

disinformation is created and evolves unchecked. As regulation of platforms expands and profitability of carrying political speech comes under question, the massive platforms may retreat from trying to be engaged in public affairs and - if unchecked - unwind their trust and safety processes.

KEY TAKEAWAYS

- Our ability to predict technologies and techniques are limited, however, we can trust that various parties will be motivated to wield them in harmful and self-interested ways.
- There is a broad consensus between election practitioners, information integrity practitioners and the general public that **information pollution is a material concern to elections across the world**, with many countries already believing it to have had a deleterious impact upon their elections. They also agree there are insufficient protections in place to challenge its impact.
- Online information pollution has offline and historical analogies, and their potency is frequently **rooted in broader grievances**.
- However, the **internet**, and particular social media platforms, have a set of features which can **amplify information pollution** in ways beyond **legacy media and traditional information distribution methods**.
- The **election period introduces additional characteristics** which further complicate the information ecosystem. The spike in political activity, the broad and partisan public stakes, international interests, high stakes to candidates and votes alike, a requirement for plurality and inclusion of political speech, and the need to provide a level playing field, are just some of the features.
- The election also introduces a number of specific **targets** for information pollution campaigns, including the **election management body**, and the election process itself. Credible elections have always relied upon the perceived legitimacy of the administrative institution and its work, which can be unduly undermined by information pollution.

WHAT IS ELECTORAL INFORMATION POLLUTION

Information pollution is a term to capture the various types of harmful information known as disinformation, misinformation and malinformation. Its various forms are characterised by a number of features.

Chief amongst these is the intent of the creator - if it be a genuine error or if it is intended to deceive. The location of the creator – domestic or external – has a material impact upon the nature of the attack and the possible responses.

Assessing the impact of information pollution within elections contributes to a better understanding of it. Information pollution facilitates direct interference in candidates and political parties, impinges on the legitimacy and credibility of electoral processes, and may even lead to suppression of votes.

From modern technology have sprung forth tools which can be used for progress and peace, but also as weapons and threats. A range of risks have been experienced in the field that threaten the integrity of the election process and the ability for all stakeholders to freely participate. These calls for a broad view of the threat landscape.

Within this document, are a myriad of ways the digital age has reinforced or introduced new dynamics to electoral processes. These phenomena are inextricably intertwined, calling for a holistic consideration of digital threats to elections, and how they can be averted. Looking forward, threats will inevitably grow as practice innovates and technologies emerge, not least artificial intelligence.

A number of
inter-connected
concerns
are below,
however
viewing them
in silos is likely
to overlook
how threats are
conducted in
practice:

- **Hate Speech and Incitement of Violence** – A related concern is the potential the internet provides to spread hate speech targeting vulnerable groups and the incitement to electoral violence. Often, further complicated by the algorithmic nature of platforms, and user anonymity.
- **Foreign Information Manipulation and Interference** - The EEAS defines FIMI as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.
- **Cybersurveillance**: Politicians and civil society have been targeted by sophisticated tools designed to infiltrate their phones, allowing access to personal data, microphones, even cameras. These tools have become so advanced that they can even be deployed without the user having to take any action (so called zero-click exploits)
- **Censorship**: The internet provides a host of new means to censor information. Governments may have undue ability to censure online activity, while platforms are placed to conduct effective and opaque censorship.
- **Internet Shutdowns**: The power to turn-off online services, or the entire internet, can be wielded to repress political dissent and remove the means of organisation. While there may be legitimate reason to take such actions, there are concerns that they are more often deployed for political advantage.
- **Privacy Violations**: The digital age has brought forth vast stores of personal data, which can be used to profile people, support influence operations, or extort individuals.
- **Cyberattacks**: Cyberattacks can be deployed to disrupt or infiltrate electoral services, expose personal data or extort people.

KEY TAKEAWAYS

- There are a range of digital threats to elections, and while information pollution is a considerable one, it is not alone. Other examples include, censorship, internet shutdowns and throttling, cybersurveillance, privacy violations and cyberattacks.
- Within this document, are a myriad of ways the digital age has reinforced or introduced new dynamics to electoral processes. These phenomena are inextricably intertwined, calling for a holistic consideration of digital threats to elections, and how they can be averted. Looking forward, threats will inevitably grow as practice innovates and technologies emerge, not least artificial intelligence.

EEAS RESPONSE TO FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI)

For the EEAS, FIMI presents a dual challenge. On the one hand, they are involved in the protection of the EU's and its Member States' against foreign interference. On the other hand, they exchange experience in fighting FIMI with partner countries within the EEAS framework of democracy promotion efforts and civilian and military missions and operations. This duality is reflected in the work objectives of the EEAS Strategic Communication division (SG. STRAT.2).

To address these challenges the EEAS has been working with other European institutions, Member States and international partners, as well as civil society and private sector stakeholders. Through the multi-stakeholder approach, they aim to improve the EU's resources and capabilities to prevent, deter and respond to all types of FIMI regardless of the source and the region it occurs.

In its work, EEAS combines policy and methodology development, analysis and responses to FIMI, covering the entire cycle necessary to address FIMI in a comprehensive manner, such as:



One of the flagship projects of the EEAS strategic communication division, and specifically the Task Force East is the [EU vs disinfo website](#). It was launched in 2015 and has identified, analyzed and responded to disinformation in various shapes and forms.



ARTIFICIAL INTELLIGENCE AND THE ELECTORAL INFORMATION ECOSYSTEM

The role of artificial intelligence in electoral information pollution is front of mind for most experts and administrators alike. Given the existing concerns over the role of information pollution within elections, it is not surprising that the forthcoming waves of artificial intelligence would pose deep consternation, even existential fear. At the same time, there remains a limit to our collective understanding of what AI is, and will be.

With generative AI - software that can create highly convincing content – entering the public consciousness, experts are still grappling with what this will mean for information pollution. These tools have made the production of disinformation easier, cheaper and scalable. Troll farms staffed by scores of humans with the required language and cultural skills can be replaced by machines and handful of operators. AI generated images, videos and 'recordings' can be created and strategically deployed to discredit

political opponents or the election process itself. The increasing effectiveness of these tools make the produced content hard to discern as synthetic and more capable of achieving its intended behavioral influence. AI may be used to aid in the distribution of information pollution, used to create fake accounts, post comments and target content. While AI may allow the creation of infinite amounts of information pollution, what this means in practice is still being evaluated. There are a host of questions to be answered, just a few are: Can content be effectively distributed and targeted? To what extent with AI countermeasures detect inauthentic or prohibited content and behaviour? What is the impact of AI generated content or deepfakes on voter behaviour? What types of authentications approaches are there for synthetic media – such as labelling - and do these redress the influence on the voter?

Generative AI is in the zeitgeist, but is only one AI branch. Others are also developing at breakneck speed. AI's form will be determined by various forces and decisions. The open or closed nature of AI models are expected to have a tangible impact upon the inclusiveness of elections.

Two broad views of how to constrain the potentially harmful impacts of AI were discussed in Brussels. There are urgent calls for an effective AI governance architecture. For those who advocate regulation, statements by industry leaders calling for governance are now matched by their actions. Some feel that the latest form of generative AI which digital firms are rushing to produce, are done so with little consideration to their potential impact and erosion of electoral processes.

A critical view put forward reads that governance will ultimately be found lacking and a technological arms race is called for, with the solution to a 'bad' AI being a 'good' AI. If this is the case, then a host of new questions emerge, such as how to build positive AIs that can defend the integrity of elections, who will control these models, how to put these into action, what are the constraints around computing capabilities, to name just a few. AI is also being deployed to identify fake content, however it is an arms race that may not be winnable. Worse still, the mere potential that otherwise convincing content can be fake has the potential to undermine public trust.

The myriad of concerns discussed above should not blind to the potential benefits that AI technologies may hold for inclusive political competition and broader societal questions. As much as investment and policies are needed to protect against harms, efforts are also required to leverage advantages. For one, UNDP has deployed forms of artificial intelligence to assist in the review on online content in its information integrity efforts. Looking forward, more powerful AIs are posited to have more powerful predictive to assist in preventative efforts, for example, identifying potential hot spots of violence against women in politics.

GENERATIVE AI

Generative artificial intelligence is a form of artificial intelligence which can generate various types of content, such as text, pictures, videos and other media, based on user commands. They are trained using large sets of data which they use to predict how to satisfy the user request.

KEY TAKEAWAYS

- **Artificial Intelligence** is preoccupying the electoral and disinformation communities, as it is many other fields. Artificial Intelligence is expected to have a transformative influence upon much of modern life, and elections are not exempted. Generative AI will make the production of seemingly authentic and evocative harmful content easier, cheaper and more scalable. AI may also be deployed to support the distribution of information pollution, including through the creation of fake accounts or facsimileing convincing engagement.
- **Building protections against the weaponization of Artificial Intelligence** in electoral information environments is vital but complex, with defenses likely to incorporate regulatory, educational and technological approaches. There is a need for international cooperation given the global nature of the issue.
- **Artificial intelligence** also promises to support the integrity and inclusion of elections, both as a counter measure to adversarial AIs, but it may also hold **create new opportunities** for greater participation, voter information and equal competition.

THE IMPACT OF DISINFORMATION ON ELECTION PROCESSES: COUNTRY CASES



LIBYA – The Chairman of the High National Electoral Commission stated that the failure to deliver elections in 2021 was rooted in widespread disinformation, enabled by the ease and impunity by which it can be spread, by individuals and platforms alike. He also expressed reservation on the role of media in promoting a healthy information ecosystem, in an environment where the incentives are towards creating partisan and attention-grabbing content.



KENYA - In Kenya, the 2007-08 electoral violence, rooted in disputed elections and tribal divisions, was fanned and facilitated by text messaging, making clear the interplay between digital communication, media environments and political polarisation. A decade and a half later, the elemental issue of technology and its disruptive impact on electoral processes remains the same, despite the advances in technology that render this disruption more sophisticated and destructive. Despite significant progress, more recent elections faced various challenges, including: gendered disinformation against female political leaders, polarisation and divisive rhetoric, on-going security concerns, and the limited capacity of Kenya's EMB to handle disinformation.



ZAMBIA - The 2021 General Election faced an outbreak of disinformation and misuse of social media, in particular attacking the Zambian Electoral Commission. Ordinary citizens were also targeted, to discourage their participation.



DEMOCRATIC REPUBLIC OF CONGO - The media landscape is highly monopolised by political elites and religious leaders. Public broadcasters and the Conseil Supérieur de la Communication face political pressure, while internet shutdowns which are now commonplace are feared to also afflict future elections. Some positives were identified, however. Local radios are present across the DRC, playing an important role in the dissemination of local news and having greater impartiality credentials than the major national media outlets. An example of such would be the 'initiative des informations' by youth in Goma.



BANGLADESH – Information pollution has had a direct impact on the decline of the democratic processes in the country, with online information pollution intensifying in advance of the 2024 Elections, with a reported increase of over 60% in the last three months. Online outlets are deploying disinformation to target opposition parties. Despite fact-checking in country, the content-level approach is insufficient in addressing the concern.



DYNAMICS OF ELECTION-RELATED VIOLENCE

A central concern for almost all electoral stakeholders is how to prevent election-related violence. Unfortunately, for some, violence is a means to further their political fortunes. Election violence remains a common phenomenon across the world. Yet, understanding the motives and techniques of the producers of violence can inform mitigation approaches.

Within the context of an election, violence can be used as a tool of exclusion or inclusion. Contestants may benefit by using violence and intimidation to discourage a particular group or constituency from participating in elections. More active forms of exclusion may involve denying access to election services, such as voting centres. On the other hand, violence as a tool of inclusion may be less noticeable but no less potent. Political leaders may portray violence as a necessary form of self-protection vis-à-vis another community, group or constituency, thus mobilising voters who otherwise might not be as involved or inclined

to vote. Typically, both forms of violence rest on leveraging existing grievances and perceived injustices against a perceived rival or foe.

Another perspective on the dynamic is rooted in a potential mistrust between those who organise elections, and those who participate in them, i.e. political actors. This mistrust leads political actors to denounce the legitimacy, credibility and transparency of election processes even before they are concluded, with parties reporting manipulation and fraud before results are known. This feeds into post-electoral violence by aspirant political actors and agitated supporters.

Institutional constraints play a fundamental role, as electoral violence is generally more overt and widespread when the executive is weaker. Similarly, where the state and its organs function effectively and inclusively, there is a greater chance of peaceful elections – for example, the efficacy of election-dispute resolution mechanisms.

The role of the digital age in these dynamics is a matter of on-going concern. Misinformation feeds, exacerbates and foments election-related violence, leveraging pre-existing grievances. Election-related violence and misinformation far predate the digital revolution, however, these new technologies have provided new fora for electoral violence to exist, and for violent strategies and drivers to be propagated. Effective disinformation rests upon the ability to spur an emotional response, a task to which social media has proven adept. Furthermore, the nature of digital channels have made governance of the electoral campaign more complicated and opaque, when compared to traditional media.

KEY TAKEAWAY

- Political actors have long deployed **electoral violence** to advance their electoral interests, often using disinformation as a tactic to mobilise their supporters, undermine their opponents, or promote false narratives about the electoral process. There are concerns that the internet, and online platforms, have provided an under regulated yet potentially powerful medium to instigate electoral violence with few, if any, consequences. There is also a fear that major platforms are designed with the goal of maximising user engagement. This includes elevating content designed to trigger emotional responses, which in turn potentially contributes to electoral violence.





PROTECTING THE ELECTION INFORMATION ECOSYSTEM

Posing such numerous and significant challenges, the digital age demands a new family of activities designed to protect the various stakeholders and the election process itself. It is fair to say that as a community – be it electoral or information integrity – developing a clear understanding of what works and what does not is a work in progress.

When it comes to how to respond a multi-pronged and multistakeholder approach is needed. Various experts and practitioners recognise the need for a strategic approach, where the election management body would be one of the actors involved in the design and adoption of a broader plan. Information sharing and close collaboration between a diverse set of actors holding different strengths and constituencies – such as; online platforms, governments and civil society – underpin any toolkit of responses to combat information pollution. Structures can be created to allow work in concert and support coherent

and coordinated activities related to promoting information integrity. These mechanisms may come in the form of coordination bodies, loose information sharing groups, communities of practice, or more formal arrangements to collaborate on specific activities including agreed interpretation of data, the prioritization of issues and organising collective responses, to name a few. Furthermore, to really understand the effectiveness of different responses, building structures that permit research and learning are vital.

The electoral authorities, other governmental bodies, civil society, platforms, academic, the media and the political contestants are the key actors involved in the electoral information space. Each holds the potential to strengthen or weaken the information environment, through their actions, or inaction. For example, the EMB is the target of information pollution, but also has a

vested interest in protecting work within its mandate by providing access to reliable information on the election and having the capacities to combat disinformation narratives intended to deter participation or undermine its credibility. The role of powerful tech companies cannot be underplayed, as they provide the systems and platform where violence takes place. These companies need to work together with national EMBs in the context of elections to ensure their inclusivity and information integrity.

Furthermore, multi-stakeholder approaches can permit the sharing of knowledge, and a greater capacity of advocacy. For example, EMBs may not always be best placed to address certain narratives about the elections and partnerships with fact-checking organizations could address any potential conflict of interest and/or capacity challenge EMBs may face.

Such approaches may fit within a broader country plan for disinformation and hate speech. Where possible, the responses should be guided by a strategy – a strategy which may complement a broader national vision of how to tackle the challenges of information pollution. These may be plans for the governmental institutions, or a broader multi-stakeholder vision, depending upon the realities of the context.

Three families of approaches have been identified, each with their own benefits and limitations -and with invariable overlaps. How they are applied is a contextual decision. No one size-fits-all solution exists, instead each country needs to define its own mix, and each programmatic actor needs to decide how it can best contribute.

When designing the approach, consideration should be given to the nature of the concern outside of elections. Rarely is information pollution contained only to election periods – even if the scale and stake are not as acute. Furthermore, it is understood that many of the division caused by information pollution is the result of exacerbating pre-existing grievances. These issues cannot be tackled purely within the context of an election and short term projects, but require a more longitudinal approach.



Identifying and responding to information pollution in the course of an election process - the operational process of tackling active disinformation

Approaches such as social media listening, fact checking, different content moderation approaches, strategic communication are most common. However, there is a broad consensus that content level responses are limited. While a responsive approach is necessary, the nature of the challenge means that reactionary responses are unlikely to completely undo the damage created.



Building greater personal resilience to information pollution - focusing on the educational and informational capacity building

The theory contends that by building critical thinking and public election knowledge, the public should be better equipped to resist the influences of election information. However, concerns have been raised. For example, in the context of an election process, what is the role of critical thinking when political partisanship is the main driver. Even if approaches can help the bulk of people, what about the fringe where the most extreme views thrive.



Regulation of the information environment and political actors to constrain and disincentivize the propagation of information pollution

Regulation is considered to be vital towards inducements for producers to not create or spread information pollution, and intermediaries – platforms – to prevent it. There are a range of approaches, including voluntary and binding guidelines, from supranational to extremely local. Fundamentally, attempting to engage the political actors and media in contributing to the healthy information ecosystem can be extremely beneficial, however, we also heard about the various challenges in convincing people to act against their own short-term interests - political and financial.

KEY TAKEAWAYS

- The digital age poses numerous and significant challenges to the electoral information environment, demanding **a new family of activities** designed to promote information integrity and protect the election process.
- The electoral authorities, other governmental bodies, civil society, platforms, academic, the media and the political contestants are the **key actors involved in the electoral information space**. Each holds the potential to strengthen or weaken the information environment, through their actions, or inaction. The role each actor has to play is guided by the various contextual factors, such as mandates, capacities and the political dynamics.
- EMBs and the processes they oversee may be victim to information pollution. To be better able to respond to such concerns, EMBs with capacities to identify and counter information pollution, and communicate timely and accurate information to the public may be better able to support credible elections.
- Because of the complex nature of the challenge, effective responses to information pollution require a holistic and systemic approach with a diverse set of actors holding different strengths and constituencies. A recommended approach for actors in this space is **multi-stakeholder engagement**, establishing structures which allow them to work in concert and to be coherent and coordinated in the various activities related to promoting information integrity. These mechanisms may come in the form of coordination bodies, loose information sharing groups, communities of practice, or more formal arrangements to collaborate on specific activities including agreed interpretation of data, the prioritization of issues and organising collective responses to name a few. Furthermore, such engagement will permit the sharing of knowledge, and a greater capacity of advocacy. For example, EMBs may not always be best placed to address certain narratives about the elections and partnerships with fact-checking organizations could address any potential conflict of interest and/or capacity challenge EMBs may face.
- Where possible, the responses should be guided by a **strategy** – a strategy which may complement a broader national vision of how to tackle the challenges of information pollution. These may be plans for the governmental institutions, or a broader multi-stakeholder vision, depending upon the realities of the context. Strategies are expected to be inline with international human rights law, and designed around the country situation.
- While there is a spike in information pollution during the operational and campaigning period directly preceding an election, a more **longitudinal vision** is important to address increasingly protracted attacks on electoral institutions that are pre-emptive as well as well financed, informed and organised, and strengthening broader resilience in advance of the peaks, which takes time to establish
- When conceptualising a program of activities, a **framework** can be developed on 1) how to **detect and respond** to information pollution during the election 2) how to build the underlying **public resilience** to information pollution, 3) how to **regulate** the landscape to deter actors from disseminating information pollution and platforms for facilitating it. More detail on each can be found on the SELECT website [Information Integrity Report – Select \(sustainingpeace-select.org\)](https://sustainingpeace-select.org/)

SELECT Sustaining Peace During Electoral Processes

Global Conference PEACEFUL AND IN ELECTIONS IN A DI

Sharing challenges and ic
programmatically solutions.

<https://www.sustainingpeace-select.org/>

IDENTIFYING AND RESPONDING TO INFORMATION POLLUTION

A healthy information ecosystem is vital for genuine and credible elections. What this looks like has been transformed by digital media. The very nature of what speech and tactics are permissible within an election are shifting.

As the information ecosystem around an election is to be protected, the first step in addressing disruptive elements is to identify them. Yet, finding actionable information pollution is as important as it is difficult. In the course of an election, the scale of content – permissible and restricted – can be massive. This task has been further complicated by artificial intelligence, with phenomena such as deepfakes and interactive AI material proving difficult to distinguish from genuine content.

The foundational activity when it comes to responding to information pollution is fact checking, in its various iterations. Conducted by impartial civil society, fact-checkers monitor various forms of media, often assisted by technological tools. Despite some successes, there remain some underlying concerns around the full efficacy of fact-checking. Redressing the impact

of false narratives, especially when it's limited to labels, can be limited. Engaging audiences in debunking is challenging. Other problems include suspicions about potential bias of fact checkers – either legitimate or a tactic to delegitimise their work.

Enacting better partnerships between interested parties is expected to increase capabilities and reach of corrections and should be a priority when looking to establish an impactful program. For example, sharing of flagged content between different monitoring actors can reduce the overall burden. Partnering with groups with greater public reach or legitimacy can improve the efficacy of corrections.

The traditional media have a vital role in reporting upon the election and impartially communicating to the public. Part of this duty may include holding politicians to account, scrutinizing claims, and challenging disinformation. Increasingly, media houses are engaged in a form of fact-checking, building relationships with other actors in the field, and using their audiences to communicate

corrections. However, the ideal of an impartial and universally trusted media has been strongly questioned, with concerns that some outlets may be guided by financial or political motivations. In particular, within highly politicized contexts, considerable caution may be warranted.

Governments must take information pollution seriously and themselves establish structures to combat it. Within an election, this may involve the monitoring of the electoral campaign. Proactive adoption of policies to counter misinformation and disinformation, promote digital media education, should be done but not at the cost freedom of expression or for political gain. Concerns have been described that in some countries, the governments influence over the information ecosystem be wielded to support the incumbent political party.

Some of these governmental activities may be assumed by the election management body. As a direct target of much information pollution around an election, their tools to understand the information environment and deploy strategic communications, and lead on voter information are powerful defensive competencies, for the institution and the electoral process.

Platforms should assume their responsibility towards a healthy information ecosystem. Within this, they should deploy adequate content moderation teams and enforce appropriate policies. With much of the distortion of online narratives being at the hands of malicious actors, the disruption of coordinated networks should be an important part of their work. They also have more enabling work to do, such as provide access to data, support civic engagement and enact transparency measures around political advertising.

However, many remain concerned that platforms are not doing enough. As intermediaries, they wield vast power and wealth, however their interest and investment in electoral integrity has been found to be wanting in some countries. In other contexts, there was praise for their work in supporting election management bodies. During the conference, both international experts and national authorities called on platforms to do better, and to do so across for all countries alike.

Complementary to these national endeavours, a global, comprehensive effort is needed to address electoral information pollution, which can contribute to a better understanding and identification of the phenomenon. Some have called for a global body dedicated to the monitoring and reporting of information pollution trends.

KEY TAKEAWAYS

- Identifying and responding to information pollution in the course of an election process is a critical area of work when attempting to defend an on-going election. Approaches such as **online content monitoring and analysis, fact checking, open source investigations and strategic communication** are common.
- There may be various actors charged with defending the electoral information environment. Part of this responsibility is to monitor the information environment and effectively address harmful content and narratives. However, there is a broad consensus that **content level responses are not sufficient**.
- Fact checking, as an activity typically delivered by civil society, media and other civilian groupings, is a vital and popular activity around election processes. However, its limitations in reaching and affecting the views shaped by information pollution need to be acknowledged. In turn, these limits inform which complementary actions are selected, designed and delivered.
- Election management bodies are well advised to invest in tools and structures including partnerships to better understand and respond to the information environment, as well as develop their strategic communications competences to better defend their staff, the institution, and the election process from malicious actors.

SIERRA LEONE FACT CHECKING



most of the time the contaminated content aligned with the electorate's positions, together with the fact that politicians had a tendency to misinform and deploy false facts in order to win votes. Yet the iVerify project, focusing on fact-checking misinformation and disinformation and getting the facts across to the electorate, had proven a success during the June 2023 presidential election in Sierra Leone. The following procedure was the one carried out by consortium led by the Sierra Leone Association of Journalists. iVerify managed a fact-checker software and a network, which after the fact-checker results were published, disseminated the facts. This allowed to highlight and expose false and unproven information, which in turn allowed to identify sting influencers on social media.





BUILDING PUBLIC RESILIENCE TO INFORMATION POLLUTION

If the influence of information pollution upon a society is to be reduced, a key approach is to make the public less susceptible to electoral information pollution.

When considering how to approach resilience programming, it is important firstly to think about who is most susceptible to information pollution, bearing in mind that the most vulnerable will vary depending on the specific context. Therefore, any foundational landscape analysis must be adapted to local contexts.

Some types of approaches that fit within this area of work are:

Digital Media Literacy: Increasing digital media literacy and critical thinking skills of the public is thought to be an important step in supporting people to navigate the online – and offline – information ecosystem. So far, 30 countries have

adopted strategies on media information literacy, or are in the process of doing so, yet this number is far from the scale and ambition required at the global level.

Civic Education: Broad and effective public awareness campaigns on the election process are essential components of any successful election. Building a broad public understanding of the electoral process can prevent gaps which can be filled with information pollution. In the digital age, they can be designed to increase the public's resilience to information pollution. As much as there is access to correct and credible information in the public sphere, the less influence false information can hold. However, how this can be done effectively may require careful consideration.

Media Strengthening: Citizens deserve, and require, access to reliable information. And while the election management body has some responsibilities in this area, there are parts of the political campaign that are typically out of their remit. Here, the media typically is looked toward to fulfil this role. This position is in some cases undermined by scepticism towards media and journalists. The proliferation of online advertising and the ensuing revenues also threaten to negatively impact the impartiality of online content.

One goal in this area of work is to finding ways to increase the availability and consumption of local media, as well as the development of independent and reliable public media. It provides a proactive counterpoint to the more reactive approaches to information pollution. It is hoped, though there remain some concerns, that local grass roots media may be less political or potentially not captured by political elites.

Within these types of activities, there are a myriad of different approaches. Creativity is important in designing effective interventions. Ensure lessons are learnt from these programs is vital to furthering the practice. The efficacy of different types of public resilience work are not well understood. If the electoral community is to understand what the most impactful types of activity will be, a structured approach to gathering and comparing evidence is required. With many literacy programs taking years to deliver and come to fruition, a clear research agenda is required.

Which channels are best for communicating information to the public requires context specific deliberation. In some context, public mistrust of mainstream media is common, with controlled by elites was raised in the discussion, as well as the impact of disinformation on increasing the public's anxiety. Platforms are powerful actors in changing public behaviour and spreading educational information.

Ultimately, while these approaches are important, it is not reasonable to place the burden of analysing and policing the internet entirely upon individuals. States have a responsibility to their citizens, platforms to their users and media to their readers.

KEY TAKEAWAYS

- Efforts to build greater personal resilience to information pollution can focus on **building public digital skills and education**. This stream of work can mitigate weaknesses in content related approaches.
- **Civic education** has been a long-standing activity within the election process. Spreading accurate and engaging information can pre-empt attempts to spread misleading or harmful narratives. However, this field should be expanded to build voter awareness of and resilience to potential information pollution campaigns.
- Enhancing **digital literacy and critical thinking** are vital to building broad public resilience to modern information pollution. It is an area of work only recently gaining popularity, yet its impact is still being ascertained. Ensuring rigorous accompanying research and evaluation is important to allow the community to understand what works.
- Building an **information ecosystem which provides reliable and trusted information** is vital and can be approached by various means. Closing the news/information gaps can be attempted by supporting independent local and community media, promoting journalistic capacities and building public interest media. The election management body, civil society, and the media can all contribute to this effort. Depending upon the country dynamics and the activity under discussion, different actors may be better placed than others. EMBs in particular are encouraged to adapt to the new information reality, build teams, budget for disinformation resources and capacities, etc.

HONDURAS: BUILDING INFORMATION INTEGRITY IN A POST-ELECTION VIOLENCE CONTEXT



In light of the election-related violence of 2017, in which **30 citizens lost their lives**, Honduras adopted a national policy to counter information pollution. It was centred around three actions and based on the experience from the 2021 electoral cycle.

These areas were

cyber-resilience

local community engagement

soundproofing (?) electoral bodies, accompanied by a public awareness raising campaign

More than 2000 international journalists were accredited to help national media in increasing its accuracy and countering information pollution. The EMB prompted a peace agreement between all candidates and political parties, which included an agreement to respect the 'Comision Nacional Electoral' authority to declare election results.

Despite these efforts, **1.2 million Honduras fell victim to disinformation**, highlighting the progress that remains to be made.

In order to better negotiate with large technology firms, some authorities are looking to band together. For example, in Latin America, the 'Comision Nacional Electoral' of Honduras, 'Oficina Nacional de Procesos Electorales' from Peru and 'Union Interamericana de Organismos Electorales' (UNIORE) have agreed to work together.

LEBANON: COMBATting A POLARIZED INFORMATION ENVIRONMENT



In Lebanon, civil society has expressed fears that sectarian forces have successfully co-opted the digital sphere to deploy polarising narratives and divisive speech.

The Samir Kassir Foundation is working to counter these narratives in the digital sphere. Part of their approach is to conduct monthly social media monitoring activities. Based on this, they select narratives to delve into and understand real world impact. Their findings underscore the extent to which cyber armies have orchestrated campaigns to promote hateful discourse and foster a polarized environment. These divisive approaches rely upon, and highlight, the deep rifts within Lebanese society.

The Foundation noted scaling up support for independent media outlets as important activities, but also highlighted the limitations when faced with the imbalance in power dynamics and disparities between these outlets and the political actors entrenching the status quo in Lebanon.



APPROACHES TO REGULATING POLITICAL SPEECH AND INFORMATION POLLUTION

The area of regulation has been considered a vital part of nurturing a healthy information ecosystem. Within the electoral context, regulation has a number of goals, namely to ensure a level playing field, protect freedom of expression, and to prevent hate speech and incitement to violence.

The manner of regulation, and the targets, remain a matter of discussion. While not a binary choice, the centrality of platforms or political parties in the regulatory approach is an important consideration. Traditionally, within the regulation of the electoral campaign, there have been constraints on the speech – both in terms of content and quantity. However, the precedent of applying such approaches in the digital age have caused some to want to explore other approaches. The alternative approach has been to regulate the gatekeepers of the online information ecosystem, to compel them to police speech.

Despite the various concerns around a regulatory vacuum around platforms, the protection of freedom of expression remains paramount in

the electoral information ecosystem. These concerns are most acute in contexts vulnerable to authoritarian tendencies where the powers could be used to subvert individual rights and advance political interests of incumbents.

Currently there are over 70 national pieces of legislation dealing with regulating online political speech, yet there is an absence of a global multilateral framework. As such, a number of attempts are being made to provide guidance on governance, for example by UNESCO in the form of Guidelines for the Governance of Digital Platforms or through the UN Code of Conduct for integrity of media platforms.

Regulatory action, an area which the EU has heavily invested in, through the Digital Services Act and AI Act for instance, has proven to be a practical approach. However, the ability to impose strong constraints upon platforms may be dependent upon the profitability of the territory – leaving many in the global South to express feelings of impotence.

There remains a concern that not all regulation is intended solely to support the integrity of the information environment, in fact, there are valid concerns that governments may use the approach to advance their electoral prospects by capturing power over the online ecosystem. While the aforementioned international guidance approaches are intended to limit this type of abuse, their influence and protections are yet to be understood.

Codes of Conduct are another form of regulation. They are distinct as voluntary agreements that may include political parties, media and platforms. Despite the seeming lack of teeth, they have been found to be effective, and potentially have less of a chilling effect. In some cases, they are convened by the election management bodies, but they can also be led by civil society or other stakeholders. Similar to digital ceasefires, it's an area of work that is still being explored, but positive experiences have been found – for example in Honduras.

How regulation – legislative and voluntary – is formed is as vital as what it deems to do. Best practice calls for inclusive, multistakeholder approaches, involving the platforms, government, civil society, fact-checkers and other concerned actors. Furthermore, frameworks should be grounded in human rights law, protecting individuals as they seek and receive information.

KEY TAKEAWAYS

- **Influencing the behaviour of political actors in the information environment** can provide another approach to constrain and disincentivize the propagation of information pollution. There are a range of approaches, =such as legally binding to voluntary guidelines, and from supranational frameworks to extremely local agreements. Fundamentally, coercing political actors, platforms and media to contribute to the healthy information ecosystem – either through legal or political means – can be beneficial if successful.
- Any approach to create accountability within the electoral information ecosystem should **prioritise human rights approaches**, most relevant of which is freedom of expression.
- A multi-stakeholder approach is warranted during the design of any regulatory activity. It is the right of **vulnerable groups and communities to be included** in the conversations taking place – be in at a local, national or international level.
- **Regulation of online platforms** can be used to shape the information environment towards promoting reliable information, reducing information pollution and assigning accountability to what has become a set of key actors in the election process. A word of caution is required, however, as regulatory processes are open to abuse and manipulation.
- Codes of Conduct can provide a more agile means of building guard-rails around the **activities of political parties and other electoral actors** and provide a means to avoid some of the concerns around government abuse. However, these approaches must be designed in a context specific manner in order to be effective, including consideration towards monitoring and enforcement.



EU DIGITAL REGULATION

The EU's approach to the spread of misinformation and disinformation, is a two-tier model. The first tier is based on the recently enacted Digital Services Act (DSA) and Digital Markets Act (DMA), which require online platforms to monitor risks and regulate them in order to ensure transparency and the safeguarding of users' fundamental rights. This first tier is reinforced by a multistakeholder approach, which is the second tier, involving more than 44 signatories to the DSA, among which civil society, governments and platforms are represented. This kind of collaboration and partnerships are deemed essential by the EU in regulating political speech and information pollution. Beyond its fundamental objective to create a safer digital space where the fundamental rights of all users are protected by establishing platform governance, the strength of the DSA, as per some of the discussions during the conference, is twofold: (1) it serves as a data gathering machine and (2) through its soft regulatory power as other jurisdictions are already looking at adapting and customizing the DSA to their local context realities.

Additional points raised included the focus of the DSA on increased transparency online to users to understand why content is taken down and be able to request for a reinstatement. Content moderation practices and policies should be clearly articulated in easy-to-understand language. The DSA further places limits on targeted ads and strengthens transparency, ensuring that ads are clearly labelled as such. Beyond its users, law enforcement agencies are empowered to uncover data and request for the removal of what is deemed illegal content. On the part of platforms, a range of requirements are imposed by the DSA, including the need to conduct regular risk assessments and address the risks identified.

Despite the fact that the DSA and DMA have the potential to serve as a positive example for the rest of the world, some challenges were identified including the attention and already scarce resources directed at certain 'markets' including the African continent being redirected by large platforms to be able to comply with the requirements set out by the DSA and DMA.

GEORGIA: CODES OF CONDUCT



For Georgia's Central Electoral Commission (CEC), upholding individuals' freedom of expression is an imperative given Georgia's obligations within the Council of Europe. Regulation of online speech was a delicate act, and is still evolving. In the 2018 presidential election, an ethical code of conduct was ratified by every candidate and political party, which together with a journalistic ethical code, testified to a degree of progress in regulating political speech and information pollution. The CEC is in the process of drafting a new code of conduct, yet this process is dogged by the lack of consensus over what constitutes hate speech and disinformation.



INCLUSION WITHIN THE ELECTORAL PROCESS

Building inclusion within democratic processes is the shared and collective responsibility of all stakeholders involved in elections and beyond. It sits as a fundamental priority in the pursuit of credible elections. Inclusion should be guiding consideration for all electoral stakeholders and activities, for example, in the digital era it intersects with use of technology in various fashions, as demonstrated throughout this report and during the conference.

Despite significant efforts, sustained progress in making elections more inclusive has been challenging. In some contexts there is growing resistance to these types of activities. Social norms that resist inclusion remain and prove persistent.

Women and youth continue to face barriers to their participation in electoral processes, and many forms of inclusion remain tokenistic in nature. Persons living with disabilities are similarly affected. The digital era has had a mixed impact on these dynamics. An intersectional approach is key, as are sustainable solutions incorporating a human rights perspective. While guided by international commitments, activities must be grounded in local contexts and following a consultative process with concerned populations. Another precondition to successful progress is sufficient and sustained funding, and formal mechanisms to coordinate key stakeholders and marginalized groups.

SUPPORTING INCLUSION THROUGH LEGAL REFORM AND TEMPORARY SPECIAL MEASURES

Electoral legislation established the ‘rules of the games’, and is one powerful vector for increasing inclusion within society. Reform processes are an important opportunity to tangibly increase representation within democratic structures. For this to lead to desired outcomes, building a set of advocates and establishing an inclusive process are helpful.

The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) defines Temporary Special Measures (TSMs) as measures to accelerate de facto equality between men and women. They shall be discontinued when the objectives of equality of opportunity and treatment have been achieved. The convention stipulates that TSMs are not considered discrimination as defined in the Convention.

The terms “temporary special measures” and “quotas” have sometimes been used interchangeably. Quota mechanisms are one type of TSM related to a country’s electoral system or candidate selection processes intended to guarantee or promote the representation of women or other underrepresented groups in an elected body. Other types include

- gender-targeted public funding for political parties;
- waivers of nomination fees;
- access to public media, access to public resources;
- Incentivisation of political parties with women candidates;
- sanctions on non-complying political parties.

Temporary special measures (TSMs) were discussed during the conference, and several examples were highlighted including the case of Mongolia (see separate box). While TSMs are valuable, they will always need to be matched with efforts targeted towards addressing deep rooted social norms.

For more information see: UNDP (2023) Supporting the introduction of Temporary Special Measures (TSMs) Link: [Supporting the introduction of Temporary Special Measures \(TSMs\) | Guidance for UNDP Country Offices](#)





Advancing inclusion in the Digital Era

The internet is a powerful tool to promote inclusion. Democratic participation can flourish as a result of it, allowing for increased awareness raising and community building.

Digital technology can support with the provision and sharing of information in more accessible and inclusive modalities. Text messaging and social media can expand the reach of information. Advanced technologies provide new ways of making services accessible to disabled persons. As a tool for communication and co-operation, technology can strengthening the civic space and contribute to electoral participation – especially but not limited to the youth.

The introduction of digital tools in the election administration and campaigning, designed to lower barriers, allow remote engagement and online campaigning more generally may increase the participation of female candidates and voters by not having to be present in person or by lowering the costs associated with participation.

Another feature of the digital age is an abundance of data, supporting data driven policy and programming to increase our ability to measure and iterate approaches.

Some incorrectly believe free expression and online safety are diametrically opposed. Whether it is on the basis of such beliefs, or for political expediency, this narrative can be deployed to implement laws which may impede on intrinsic and universal human rights within the digital space, including free expression. However, such approaches are firmly rejected, especially in the pursuit of pluralistic election debates.



Digital exclusion

While technology can and has contributed to inclusion at various levels, it can also have contrary results. Equitable expression in the online space is not guaranteed for all, and undermined for some. This is especially the case for historically marginalized groups. The deployment of election technology in the service of administering elections can also pose barriers to persons without sufficient online access or confidence in navigating technology.

Gains towards gender equality are being reversed, and technology may have a hand in these losses. Numerous cases have been described which demonstrate the ability for technology to be used to exclude groups or how bias within technology can compound exclusion. For example, gendered disinformation and online violence is reported as the main girls and young women do not want to enter politics. Similarly, one example cited during the conference described instagram algorithms disproportionately shadow banning or removing content of young black women.

The digital divide a feature in all contexts, the question to be asked is, how deep and how does it present itself in different communities? Some people may not have access to technology, others may not understand them, and then there are those who don't trust technology and turn away from the process. In contexts where internet penetration is limited, an overemphasis to online information can distort equity to information. Disadvantages may be greater amongst minorities or marginalized groups, including women and youth. One distinction that shows the greatest divergence in access is the rural vs urban divide.

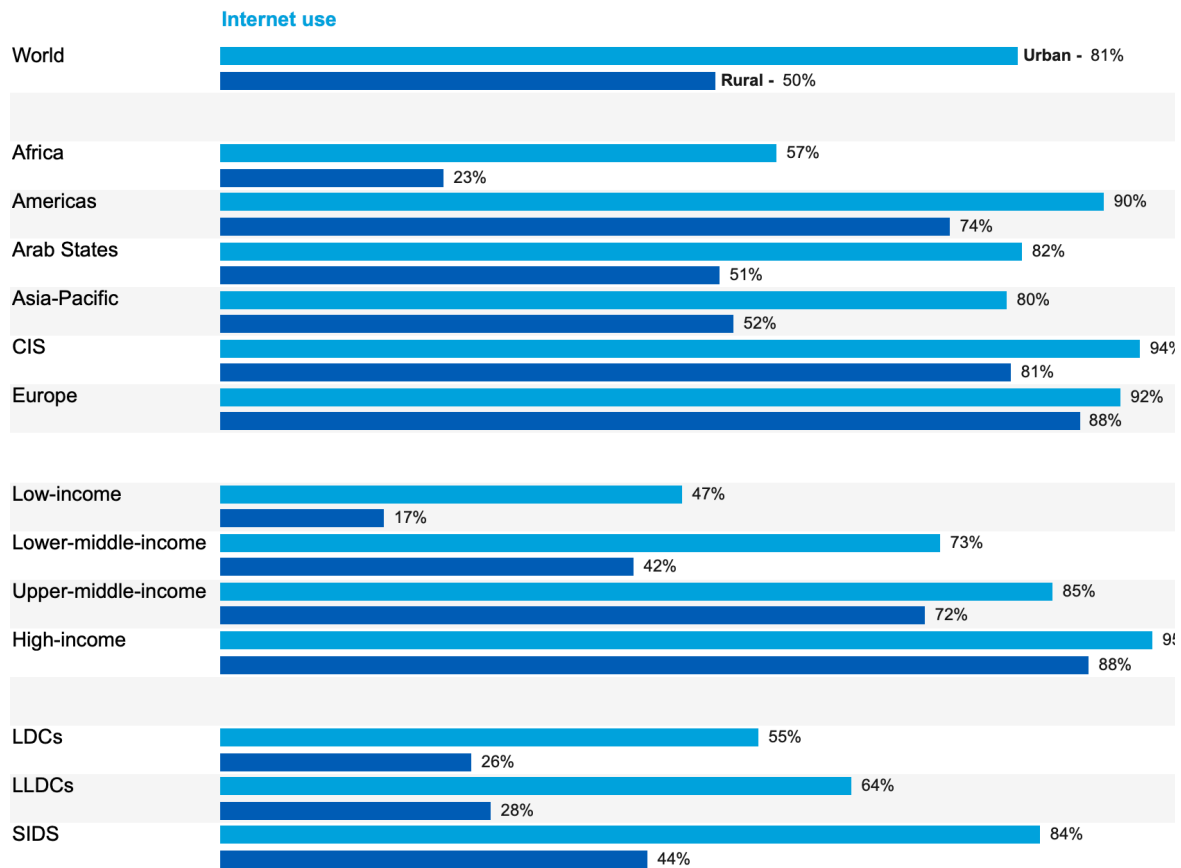


FIGURE 1: Percentage of individuals using the Internet in urban and rural areas, 2023

Source: ITU

Consequently, with every introduction of new technology, consideration should be given to less online communities, and the how impacts affect intersectional groups. Strategies should be deployed to provide equality of access and mitigate harms. This may include election administration technology, where the EMB hold primary responsibility to ensuring its appropriateness, but also broader technology around communication, where a broader set of stakeholders may look to establish activities.

KEY TAKEAWAYS

- Inclusion is a fundamental tenant in the conduct of elections, however, despite various efforts some contexts have experienced a regression in recent years.
- Democratic participation can flourish as a result of digital technology, allowing for increased means for participation and community engagement, new ways to access information and the provision of accessible election technology. Data can improve programming and services delivery.
- However, some of the observed decline in inclusion is likely to be a result of technology in the political sphere, with factors such as the digital divide, lack of trust, and systematic bias undermining inclusion.
- As technology is introduced within elections, stakeholders should consider its impact upon inclusion, paying attention to intersectionality, and designing methods to alleviate inequities – for election administration but also within the information environment.

TSMs IN MONGOLIA



The Mongolian example showcases the impact that women may have when they come together and support a common cause. It further highlights the important role that social media can play as a platform for awareness raising to bring about change. For the 2024 elections, after several attempts, there will be a 30 percent quota in place while the 2028 elections, as per the constitutional and electoral law, will have a 40 percent quota for female candidates.

INCLUSION WITHIN ETHIOPIAN ELECTIONS



In the case of Ethiopia, a number of avenues are being explored by the EMB to enhance social and political inclusion. The programmatic approach includes capacity building for the female political parties' member's caucus while the institutional approach aims to ensure inclusive measures are taken within – to practice what they preach. The strategic plan currently under development is undecided as to whether to mainstream the gender and social inclusion agenda or to have it as a separate pillar. Without temporary special measures, gender sensitive and gender responsible leaders are key.

Ethiopia grapples with low levels of internet penetration and poor digital literacy. As a result the digitalization of the electoral process and introduction of technology was only partially successful and requires a dual approach.



Sustaining Peace During Electoral Processes

www.sustainingpeace-select.org

ONLINE AND OFFLINE VIOLENCE AGAINST WOMEN IN PUBLIC LIFE

Online channels of communication offer new ways to reach, mobilise and build communities. Cheap and direct means to engage in political processes have opened the electoral process to demographic groups who previously faced daunting hurdles, be they resources, societal norms or more explicit repression. Women are one group that have taken advantage of these inclusionary opportunities, to increase their electoral prospects and voice.

However, these channels can also be abused, to serve as a means for perpetrating online forms of violence, including hate speech, repression, and fomenting the potential for real-world violence. These otherwise inclusionary tools can be repurposed to coerce women and other marginalized groups into departing from public life and degrading gender equality.

Offline violence is fairly well recognised, whereas digital violence is novel, with its own characteristics. For example, online violence is marked by a greater number of spectators and

permanence. Insults, hate speech and rhetoric can remain online indefinitely, both creating longer lasting damage, but also leaving a trail back to their perpetrator. By some measures, online attacks can be more vicious due to the anonymity and universality offered by the digital sphere. Online violence also suffers from a legal gap, which renders victims' legal redress much harder than in the case of offline violence. Often, victims of digital violence have trouble categorising themselves as such.

Existing social norms can be misused to justify violent discourses towards women. Digital processes are aggravating this phenomenon. Patterns of oppression and inequality are reproduced in the new digital realities and drive cycles of disempowerment. For example, women who require male permission to access the internet, despite having access to mobile phones. There are fears of backsliding in global norms, with even well-established principles or even language – such as the use of the term 'gender' – facing a backlash.

To understand the scale and nature of the gendered information pollution, UNDP has been exploring the use of data. UNDP has been constructing a global index of social gender norms, finding 90% of respondents held gender biases and almost half believed men made better political leaders than women. UNDP is also working to deploy artificial intelligence to develop a Gender and Social Media Monitoring Hub to monitor for real-time examples of online hate against women.

A variety of programmatic options have been developed to try to combat online violence against women, however, we are far from a resolution to the problem - if a true resolution is even possible. Part of any meaningful strategy is to address underlying gender stereotypes, social norms, attitudes, and practices that tolerate and condone such violence.

A sufficient legal framework is essential, and yet typically lacking. Most jurisdictions around the world lack legislation on online violence against women. Ecuador has demonstrated how progress can be made, where a reform of the National Electoral Law incorporated electoral gender violence, including financial and administrative penalties for engaging in electoral gender violence. Stern penalties are required, including meaningful fines, dismissal from post and even suspension of electoral participation rights. Other related legal concerns include privacy protections, such as giving women control over their own data and digital artifacts, such as images.

Examples include trainings for women in politics on how to use tools and platform features to better protect themselves online, public campaigns against online violence against women, support mechanisms to victims, escalation processes, engagement with political parties and codes of conduct. Awareness-raising activities should accompany interventions, aimed at addressing gender stereotypes, social norms, attitudes, and practices that tolerate and condone such violence, to address the root causes of the issues.

The role and capability of platforms in mitigating these harms deserves scrutiny. Digital tools should be consciously constructed in line with social needs, striving to promote their inclusive aspects and protect against their utilisation for harm. Avenues are required to allow policymakers and civil society to connect and advocate their expectations to platforms. Where required, regulatory measures may be called upon to enforce measures upon platforms.

KEY TAKEAWAYS

- Online violence against women has become an endemic concern within elections, deployed to make public life untenable for aspiring female politicians and supporters.
- The issues of gendered online discrimination are underpinned by more fundamental prejudices within societies – biases held by both women and men. Accordingly, programmatic options should acknowledge and address these underlying drivers.
- Despite the disturbing extent of abuse against women, there are a range of activities that can and should be deployed to protect them, strengthen their participation and introduce accountability ranging from awareness raising and engagement to capacity building and legislative reform coupled with enforcement strategies.

EXAMPLES OF PROGRAMMATIC ACTIVITIES TO COMBAT VIOLENCE AGAINST WOMEN IN PUBLIC LIFE

- Trainings for women in politics on how to use tools and platform features to better protect themselves online,
- Conducting public campaigns against online violence against women,
- Data driven monitoring of online violence against women and early warning systems
- Awareness-raising activities to addressing underlying norms which promote gender-based violence.
- Establishing mechanisms to support victims of online and real-world abuse
- Assistance in inclusive legislative reform,
- Supporting the design and negotiation of escalation processes with platforms and national authorities,
- Engagement with political parties and codes of conduct including appropriate provisions.

DEFINITION - VIOLENCE AGAINST WOMEN

Violence against women in political life is any act of, or threat of, gender-based violence, resulting in physical, sexual, psychological harm or suffering to women, that prevents them from exercising and realizing their political rights, whether in public or private spaces, including the right to vote and hold public office, to vote in secret and to freely campaign, to associate and assemble, and to enjoy freedom of opinion and expression.

Within an election, this can take the form of gender-biased scrutiny by media and the public, targeted attacks against female voters, and even forced resignations and assassinations of women politicians in the most **extreme** cases. Online, these acts can take various forms, such as stalking, bullying, hate speech, leaking personal information, creating false and embarrassing images and video, to name just a few. Such violence can be perpetrated by a family member, community member and or by the State.





YOUTH PARTICIPATION FOR PEACEFUL AND INCLUSIVE ELECTORAL PROCESS

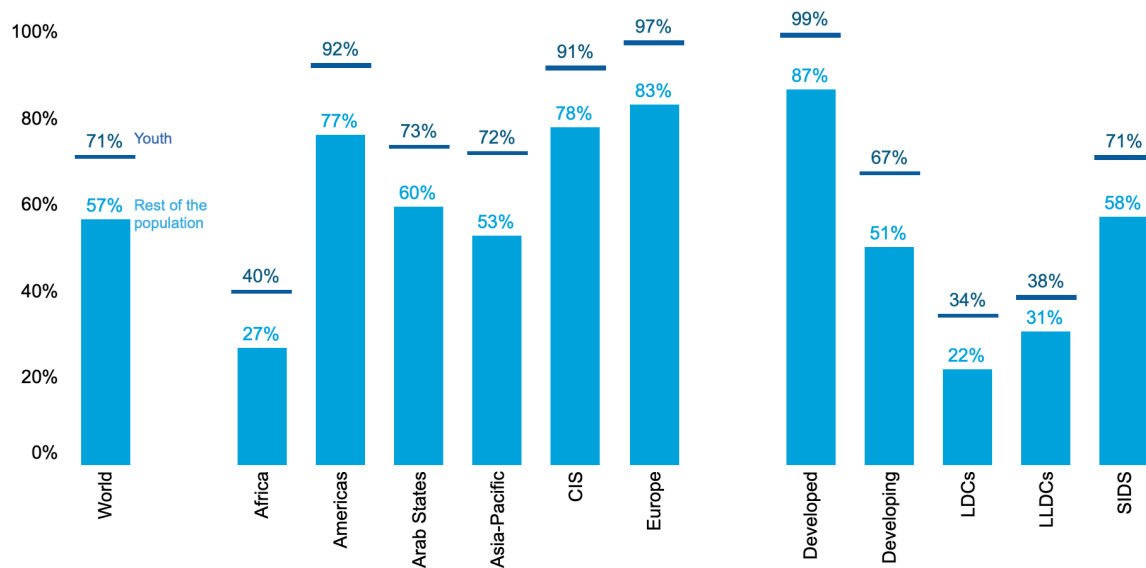
Young people make up an increasingly large share of the world electorate; however, they remain comparatively unengaged in electoral politics. In much of the world, 18–34-year-olds display a steep decline in satisfaction with democracy. At the same time, they demonstrate a great commitment to civic life, raising their voices on a number of topics, such as gender, racism, socioeconomic inequality, and rights and liberties. In particular, where possible, they tend to participate in politics through online channels.

Young people experience discrimination and exclusion, and young women are particularly affected. The stereotypical view of young people as disinterested in politics, objects of policy and troublemakers has caused development programming to largely focus on motivating young people, prior to elections, to vote while preventing them from engaging in electoral violence. Instead, we should see young people as crucial actors in sustaining peace. Unsurprisingly, programs intended to target youth require their inclusion during design and delivery. Furthermore, they should often seek to promote the voices of youth.

Transparency and trust are usually brought up whenever the topic of how to successfully engage with youth in elections is raised. Young people require protection from various online harms. The potential influence of information pollution is widely acknowledged concern, however there are a host of other cyber practices that they must be able to avoid, such as malware, phishing and, risky sharing of private information. At times, there is a mistaken conflation between having access to technology from a young age and having solid digital literacy skills. These risks restate the need for digital literacy training for school age children – and beyond.

An over-reliance upon digital as a means to engage with the youth is a mistake. Often it is not the channel which is the reason for apathy, but deeper seated political and cultural reasons. The key is to harness young people's interests, be it sport or culture, and deploy them to increase their participation and engagement in electoral processes

That being said, the channel is still relevant, especially in context with digital divides. Despite the attractiveness of technology to youth, in high unemployment countries they often are disadvantaged in terms of access.



Note: youth means 15-24 year old individuals using the Internet as a percentage of the total population aged 15 to 24 years. Rest of the population means individuals below 15 years old or over 24 years old as a percentage of the respective population.

FIGURE 2: Percentage of individuals using the Internet by age group, 2023

Source: ITU

KEY TAKEAWAYS

- It is crucial to involve youth in the design and execution of activities intended to promote peaceful and inclusive elections, in order to increase their potential for success.
- Despite the value of using technology to engage youth within the electoral process, it can be inadequate to meaningfully engage in all circumstances – especially where there is intersectionality with other attitudinal or material constraints.

UNDP ACTIVITIES IN THE YOUTH SPHERE

A core aspect of UNDP's work in Youth and Elections is the delocalisation and decentralisation of information.

In Madagascar UNDP has set up an election observatory dedicated to spreading messages of peace and prevent violence during elections.

A UNDP initiative in the Great Lakes Region supported youth-led community radio stations which diffused messages of peace and coexistence, contributing to creating a safe space where young people could discuss community and governance issues.

Another activity, the 'Generation 17' initiative, is conducted with Samsung to promote the 17 Sustainable Development Goals – the Global Goals – by equipping young leaders with digital tools in order to amplify their voices and share their experiences through the digital sphere.



UNDP DIGITAL TOOLS FOR INFORMATION INTEGRITY

The **iVerify** system seeks ensure that voters and citizens have access to verified information, via various channels, including a website, social media and radio. It does this by strengthening the capacity of national stakeholders to prevent and/or mitigate the spread of mis/disinformation by strengthening the capacity of national stakeholders in identifying and fact-checking online and offline content, around elections and beyond, with the overall objective of providing electorate and citizens with verified information via website, social media and radio means.

The **iVerify** system provides ways for citizens to actively engage in the factchecking process, by allowing them to request verifications through dedicated tiplines built-in on the website and social media. Additionally, the system allows to scrape Meta (FB, Instagram) for disinformation and hate speech using AI to increase its accuracy.

The **iVerify** platform was developed by the Brussels-based Task Force on Electoral Assistance, working with UNDPs Chief Digital Office.

In the case of Liberia, the positive impact **iVerify** had in the fight against hate speech and disinformation was extensive, allowing national stakeholders to shift from an old-fashioned model of manually checking newspapers articles and social media posts, to a system based on a software allowing much quicker fact-checking and more efficient coordination with other relevant actors. In this, maintaining the balance between speed and accuracy was essential. The Libyan experience proves how **iVerify** can create a positive impact, deterrence of electoral violence, combating historically high misinformation and ultimately contributing to credible elections.

e-MONITOR

eMonitor+ is a digital suite of state-of-the-art tools, prominently featuring artificial intelligence, which is used to **expand national, regional, and global stakeholder capacities** to promote information integrity. The suite is adept at analyzing and addressing a range of information challenges, including but not limited to mis/disinformation, hate speech, polarization, gender-based violence.

eMonitor+ collects and analyses hundreds of thousands of pieces of online content daily, spanning across platforms like Facebook, Instagram, Twitter, and YouTube, as well as website content and offline media. The system democratizes access to high-level technologies and combines them with UNDP-built solutions that are fully aligned with the UN's conceptual approach and expertise on information integrity.

The system developed by UNDP aimed to support partners to implement strategies that are evidence-based and tailored to address the unique challenges. This also includes advancing long-term digital resilience, particularly in the form of innovative policies, encouraging whole-of-society responses, and enhancing media literacy and public awareness.

In Peru, UNDP deployed eMonitor+ at the core of an ambitious multi-stakeholder strategy to expand knowledge on and dynamize joint action against information pollution. This network has analyzed more than **200,000 content and identified more than 5,000 cases of hate speech and 700 cases of gender-based violence** as used by key political actors, media channels, and thought leaders. Empowered by this new access to data and insights, more than 20 partner organizations are able to better map the rapidly evolving landscape of information pollution – transforming their action from reactive to preventive, and from individual responses to system movement.

iREPORT

iReport is a **tech tool** to enhance country-wide capacities in **monitoring, analysis and response to incidents of electoral and political violence** through the design and implementation of an Early Warning and Early Response Systems.

The main objectives of the **iReport** are to support national capacity to (1) identify and analyse grievances and disputes that could turn violent; (2) facilitate and strengthen dispute resolution through dialogue and mediation, including electoral dispute resolution; (3) coordinate effective response to situations of imminent or ongoing electoral and political violence; (4) track and analyse responses to ensure they are implemented in a conflict-sensitive and gender-sensitive manner.

The IT platform developed by the Brussels-based Task Force on Electoral Assistance facilitates the collection, collation, and mapping incidents of violence. The system draws from field reporting (via SMS, phone, website input) as well as complementary data sources. It provides the means to effectively process data, including categorization, translation, geo-localisation, prioritisation of urgency and verification of incidents.

Three guiding principles underpin the implementation of **iReport** – 1) national ownership, ensuring that the tool is fully implemented by national partners such as governments and EMBs, 2) pooling of resources, in order to increase effectiveness and find synergies and 3) sustainability, meaning that the system extends outside of election processes. **iReport** was initially deployed in Ethiopia in 2019, and since extended to Ivory Coast, Burkina Faso, Zambia, Zimbabwe, Liberia, Madagascar and Honduras.



An unclear but forward technological roadmap

Attendees to the conference were asked what types of election assistance they would welcome, and one third of responses were related to support in application of technology within election administration. For practitioners in the digital age, there is a strong interest in understanding how technology can allow them to deliver election, better.

The application of technology within the electoral administration has accelerated over years, though not necessarily in the ways expected. Since the advent of the internet, there has been an expectation that voters would soon cast their ballots online. However, despite the rapid spread of personal computing, in-person voting has persisted. Fewer than 1 in 100 votes globally cast online. Rather, the digital transformation of the

electoral process has taken place elsewhere, for example with voter registration being augmented by biometrics and integrations with civil registrations, results processes being facilitated with the internet, and the proliferation of voter information innovations.

Where online voting appears to be finding new traction is for out-of-country voting. The broad reasons this seems to be an acceptable use case is the technology has matured, conventional means of serving out-of-country voting are becoming obsolete, the covid pandemic changing norms and OCV already compromised in comparison to the polling centre experience. Perhaps most vital is that there appears to be a genuine need in terms of building inclusion amongst communities who are otherwise poorly served. And yet, even

in this case, there are strong voices against online voting, for reasons of tradition, secrecy of the vote, and concerns over security.

Regardless of the direction of digital transformation, election administration is undergoing an evolution. Like almost all parts of the corporate and public sector, the appearance of new technological tools has presented opportunities to better serve users and improve their ways of operating. In the context of an election, this can lead to a number of improvements. For example, it can offer new ways of more broadly and equitably improving participation in the election process. It can provide new integrity measures and ways of building confidence in the election process. It can have offer operational benefits which make delivering an election more cost efficient, simple and responsive.

DIGITAL TRANSFORMATION

Digital transformation is the application of digital technologies, tools and applications to enables new ways of operating, engaging with stakeholders and providing services to the public. Alongside the introduction of technology, organisations typically undergo corresponding administrative and cultural changes to support the success of the innovation.





Trust and Technology in elections

The discussions in the conference also displayed the maturity of the community, which had on the basis of hard taught lessons recognised that their support for new technology would not succeed without bringing the public and other stakeholders along with them.

Irrespective of technology, a key goal of any electoral process is to establish trust between the public, the election management body and the process they are implementing. Yet public trust is a mercurial goal, formed by various signals, norms and perspectives.

Election management authorities often convey a need to increase the application of technology in the election process, seen as a way of increasing efficiency, inclusion and a necessary result of broader public sector digital transformation. However, while contemplating digitising the electoral process, administrators need to consider how their decisions will influence public trust in eventual elections.

Implementers of electoral technological reforms have found that the most effective way of building confidence in innovations was gradual and incremental progress. Such a mindful approach to deploying electoral technology can help overcome any public wariness, including with voting technology. It is also a way to prevent or mitigate negative experiences or technical failures which can fuel public mistrust in the approach and the institutions.

The technical competence of the election management authorities, or their vendors, is vital. The correct implementation of technology is required, and naturally this will require greater digital capacity within the election management body. Various examples of the same technologies being deployed, but to differing success have been seen, with a key differentiator which influences the success of the deployment being the professionalism of the election management bodies.



Exposure to cyber attacks

When considering how and where to apply technology in electoral processes, rather than taking a maximalist understanding of technology as a replacement for all human-related factors, a less extreme and pragmatic position can be to consider how different stages of the election can be enhanced, with a vision towards a holistic upgrade of the broader electoral process cycle.

With waves of digitisation have come the threat of cyber attacks. These concerns are front of mind for electoral administrators, and voters, as they look to understand how they can deploy technologies which bolster, not undermine, the credibility of the election. In response to these threats, cyber-security is an increasing consideration when designing and maintaining systems.

Cyber-security practice is a response to a landscape of threat actors, each with their own motivations and capabilities. These actors include:

1

criminal groups and organised crime, who employ digital tools for profit – for example through extortion or paid by another party,

2

advanced groups, potentially nation-state associated, who employ more targeted and potentially highly sophisticated attacks for a wider array of purposes, such as sabotage, espionage or disruption, and,

3

hacktivists, who are typically politically motivated individuals or groups who operate under a loose structure, and which can be hard to track down. Regardless of the intent, any successful incursion can undermine public confidence in the election management authority.

Cyber-security threats can be highly potent in their destructive or intrusive capabilities. As technology has developed, they have evolved. Artificial intelligence, and other types of automation, are fuelling their capabilities to the extent that even short periods of vulnerability can be exploited.

Heavy investment is called for in building cybersecurity defences around the election. When conducted more effectively, it involves a whole of government approach, including close collaboration with police and other security agencies. How this will work in practice changes between countries, and the broader domestic cyber cooperation in place. The UK for example has a specific agency for defending elections from cybersecurity threats, which supports the election authorities. The Philippines has close relationships with the national police and bureau of investigations, as well as command structures and contingency plans. Building cybersecurity awareness may also need to target staff and voters, attempting to convince them to make decisions that contribute to electoral security, such as not sharing any log-in details. The impact of cybersecurity on the population is also a differentiated matter, with youth being counter-intuitively significantly more vulnerable to cybercrime.

CYBERSECURITY

Cyberattack – A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device (IBM, 2023 <https://www.ibm.com/topics/cyber-attack>)

Cybersecurity - Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. (IBM, 2023 <https://www.ibm.com/topics/cybersecurity>)..





The enduring digital divide

Within any voter-facing digital transformation process, due consideration should be given to technology access by the public. The overarching goal should be to enhance inclusion, not exacerbate it. Real world dynamics may confound pre-existing stereotypes, and indicate the need for impact assessments to be conducted to allow decisions to be made upon data. For example, as young people are considered inclined to make use of the digital world, there is an assumption that digitisation will increase their electoral participation. However, in many contexts, they are disproportionately unemployed, live in marginalised communities and lack opportunities, all of which compromise their access to technology.



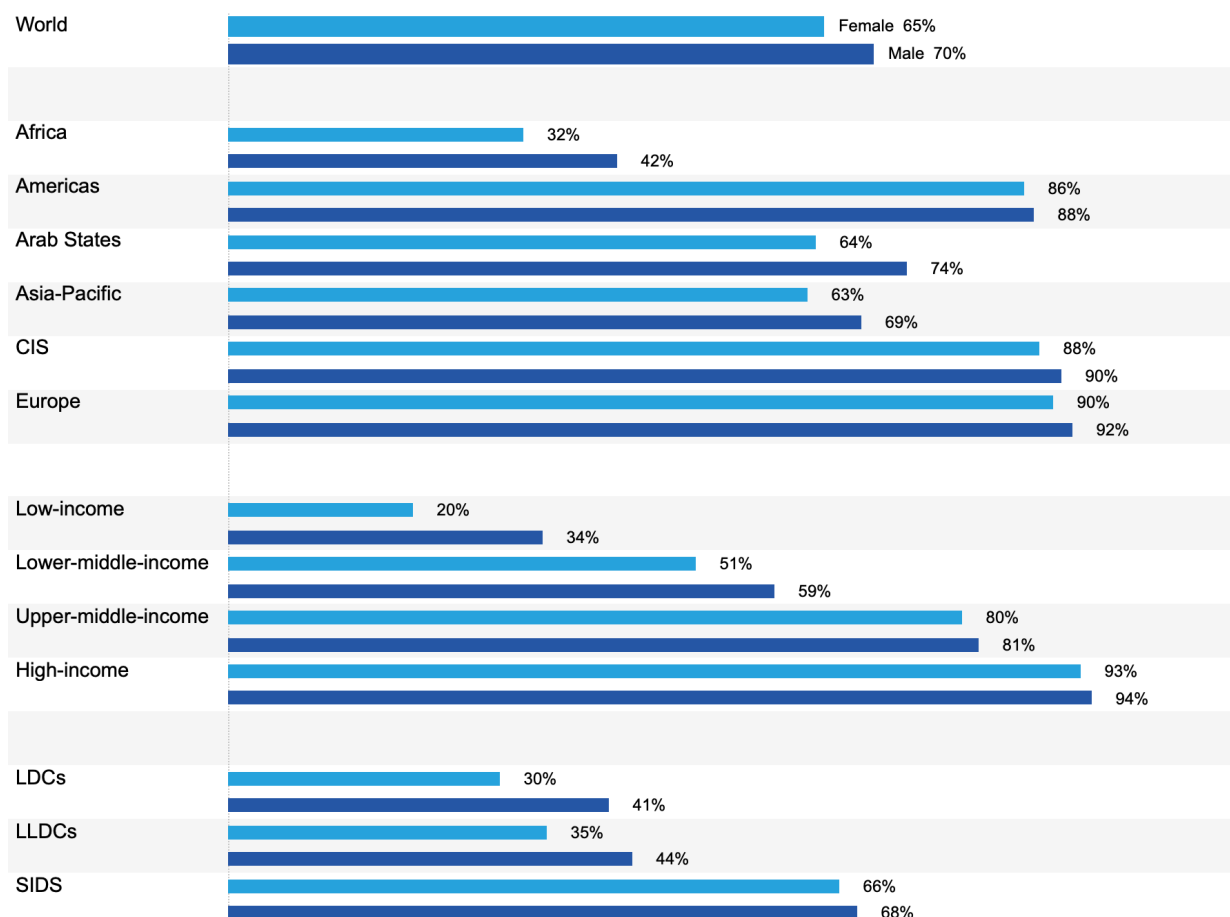


FIGURE 3: Percentage of female and male population using the Internet, 2023

Source: ITU





Artificial intelligence within election administration

The application of artificial intelligence, including the use of complex machine learning algorithms, are increasingly being explored within the context of electoral administration. Its potential is expansive, and election management bodies are only starting to explore its integration within their work.

Some initial areas under discussion are using AI as a means to organise and gain insights into electoral data, understand the broader information ecosystem, identify and combat fraud, enhance cybersecurity defences, engage with and produce content for voters, and more broadly, increase the productivity of workers and electoral technology.

Some specific types of applications have included using generative AI to construct a ballot paper and ID markers, deploying machine learning to identify fraud, training large language models as voter education agents, and using AI algorithms to enhance biometric accuracy.

Artificial intelligence presents a volatile technology. With great yet little understood power, immaturity and rapidly growing availability, it presents significant risk. These traits call for a considered approach on how they should be utilised within the electoral administration context. There are two broad risks; firstly, that the AI fails to solve the problem to which it seeks to address, and secondly, the AI operates in a way that creates unintended or deeper systemic risk.

Unintended consequences from AI applications is a vexing concern across industries. Generative AI, for example, is an imperfect agent, frequently producing outcomes that are not correct or appropriate. It's operates through opaque processes which can mask undesirable bias. Even when considering the broader application of algorithms within electoral administration, how those algorithms are designed and influence outcomes require interrogation. Many types of machine learning approaches establish statistical methods which are hard to decipher and operate in an unsupervised manner. Without a clear understanding of both the statistical approach and a deep understanding of the dynamics they are being deployed to categorise, they are more likely to fail or provide harmful outputs.

Identifying mechanism that build trust through transparency and accountability are likely important in establishing confidence in the outcomes – however in practice this can be technically difficult to convey.

This risk is reflected in the EU AI Act which calls for the application of AI in democratic processes to be treated as a high-risk enterprise – which means that measures should be put in place to mitigate negative consequences.

KEY TAKEAWAYS

- Digital transformation of election administration has been a prominent concern for election management bodies for many years, with many undertakings important reforms to make services more accessible, efficient and secure. It is an area in which a number of participants to the Global Conference reported their need for greater assistance.
- Successful digital transformation in the context of electoral administration requires approaches which prioritise the building of public trust in the technology and the broader electoral process.
- Key ways of building confidence around the deployment of electoral technology include a gradual roll out that allows trust to be established in a measured fashion. Also vital is a professional election administration capable of taking all measures possible to deliver a successful deployment, even if the scale of the initial rollouts is limited.
- Considerations about accessibility and the digital divide are expected to remain relevant for the foreseeable future. They should remain front of mind when devising new technologies intended to reach voters, or other stakeholders.
- Cyber-security is an acute concern for election administrators as they face increasingly sophisticated and varied threat actors. Building appropriate structures, engaging specialists and building strong digital capacities can provide a significant improvement in the integrity of the election management bodies digital infrastructure.
- **Artificial intelligence is of rising interest** to the community of election administrators, with hopes that it can provide important benefits to how elections are delivered. Already there is adoption of AI tools by electoral authorities seeking to enhance their work. Its application is envisaged in various aspects of their work, potentially enhancing current approaches or even transforming the nature of election administration.
- Artificial Intelligence within the sensitive area of election delivery should be approached with **due diligence**. Despite its potential contributions, it is still in its nascently, especially within the context of election administration. With this emerging practice comes a non-negligible risk, of either failure or, worse still, unintended and deleterious outcomes.

PHILIPPINES

ONLINE VOTING AT SCALE FOR OUT-OF-COUNTRY VOTERS



With **10% of the Filipino population living as expatriates**, online voting is seen as an important means of inclusion. In the 2022 presidential election, **1.7 million ballots across 93 countries** were deployed, contributing to the highest-ever expatriate vote in the country's history, with 40% of overseas Filipinos eligible to vote taking part in the elections. Internet voting was viewed as critical in increasing expatriate voter turnout. Core to the efforts of the Philippines election management body in deploying these technologies has been the establishment of a cybersecurity team.

PERU

ONLINE VOTING FOR OUT-OF-COUNTRY VOTERS



In the 2021 general election only **30% of overseas Peruvians eligible voted**, compared to over 70% in Peru's national territory. This disparity was attributed to the low capacity of the 220 consular services to service 1 million Peruvians, together with voting on election day being considered difficult due to working schedules, distance from consulates, transport, and other factors. Given the historic tightness of elections in Peru, with the last ones being decided by 40,000 votes, ensuring expatriate participation is seen as crucial. 1.7 million Peruvians were engaged through a digital vote in 2021, and the electoral commission aims for a greater share in the 2026 election by adopting a bottom-up approach, starting at the grassroots level with local communities, and eventually working all the way up to political parties and candidates. Software and electronic ID development are seen as crucial if this approach is to be successful.

KYRGYZ REPUBLIC

DIGITISING THE ELECTION PROCESS



2023 marked the introduction of electronic voting, also viewed as the solution to overcome chronically low participation both inside the country and among its diaspora population; **for local elections, participation stood at 16%, whereas only 1% of the one million Kyrgyz abroad took part in the 2021 parliamentary election**. This was considered to compromise the legitimacy of elections and acceptance of results. Looking ahead at the period 2025-27, where a number of elections are to be held, the EMB saw the opportunity to introduce Internet voting not only because 6.9 million Kyrgyz out of a population of 7 million have access to the internet, but also as a means to ensure youth electoral participation, which has waned over the years despite young people constituting the largest population cohort in the Kyrgyz Republic. Other positive recent technological innovations include the creation of an e-registration platform with the help of UNDP, where voters' anonymity and data are protected through encryption and enhanced cybersecurity. Furthermore, a digital code of conduct and training and awareness-raising centres have been established.

MONGOLIA

BUILDING TRUST IN ELECTION TECHNOLOGY



In 2012 the Election Management body introduced election voting machines to support the voting and counting process. However, a deep lack of trust in the technology led to anger and machines being destroyed. In order to build trust, the authorities attempted to introduce confidence building measures, such as parallel manual counts of a sample of stations – and when that failed, they conducted full parallel manual counts.

INTRODUCTORY RECOMMENDATIONS FOR ELECTORAL CYBERSECURITY

While there are a host of different measures that can be taken, some key recommendations include:

- EMBs should have a focal point for cybersecurity in a senior role, with responsibilities as part of their job description. This should be the basis for developing any strategy or processes around cybersecurity.
- EMBs should ensure that they have a plan and resources in place to constantly assess and resolve security issues in their platforms – in particular by applying security patches to their infrastructure shortly after they are released.
- EMBs should consider including cybersecurity concerns within their risk assessments of new services, before services are decided upon.
- EMBs should ensure that protected systems implement two-factor authentication.
- EMBs should conduct penetration testing on their systems with third parties.
- EMBs should have various plans and contingencies for when cyber incidents take place.
- EMSs should ensure cyber-hygiene training and enforcement mechanisms





Funded by
the European Union



Peaceful and Inclusive Elections in a Digital Age

Sharing challenges and identifying
programmatic solutions

AGENDA

8,9 & 10 – November 2023 – Brussels, Belgium

SELECT AGENDA AND SPEAKERS

PEACEFUL AND INCLUSIVE ELECTIONS IN A DIGITAL AGE Sharing challenges and identifying programmatic solutions

8,9 & 10 – November 2023 – Brussels, Belgium

[Link to Detailed Speaker Notes:](#)

[Speaker Notes - Peaceful and Inclusive Elections in a Digital Age .docx](#)

DAY 1



8.30 - 9.45

Registration

WELCOME REMARKS

9.45 - 10.00

Opening

Description: Welcome to participants, introductory comments

Moderator: Gianpiero **Catozzi**, Senior Electoral Advisor - Coordinator
Joint EC-UNDP Task Force on Electoral Assistance at UNDP

Speakers: A) Camilla **Bruckner**, *Director Brussels Office UNDP*

B) Gaëlle **Nizery**, *Team Lead, EU Foreign Policy Instruments
- European Commission*

10.00 - 11.15	<p>Session 2: Democratic Governance in the Digital Age</p> <p>Description: A broader view of the challenges facing democratic processes in the context of increased polarization, information pollution and digital threats</p> <p>Moderator: Meaghan Fitzgerald, <i>Head of the Election Department - OSCE Office for Democratic Institutions and Human Rights</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Tom Millar, <i>Team Leader for Democracy - Human Rights, Gender, Democratic Governance - European Commission</i> B. Sarah Lister, <i>Head of Governance - United Nations Development Programme UNDP</i> C. Katherine Maher, <i>Chairperson of the Board - Signal, Former CEO Web Summit</i> D. Meera Selva, <i>Chief Executive Europe - Internews Europe</i>
---------------	---

CHALLENGES AND OPPORTUNITIES TO ELECTORAL PROCESSES IN THE CURRENT INFORMATION LANDSCAPE

11.30 - 12.10	<p>Session 3: Information Integrity and the Challenge to Elections across the World</p> <p>Description: Discussion on information pollution in elections and future threats globally</p> <p>Moderator: Robert Gerenge, <i>Regional Electoral Advisor - UNDP, Africa</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Deborah Brown, <i>Senior Researcher - Human Rights Watch</i> B. Riccardo Chelleri, <i>EU Election Observation Missions - European Union</i> C. Simon-Pierre Nanitalamio, <i>Deputy Director - DPPA Electoral Assistance Division, UN</i> D. Karine Kakasi Siaba, <i>Political / Elections Officer - African Union (AU)</i>
12.10 - 13.00	<p>Session 4: The Impact of Disinformation on Election Processes: Country Cases</p> <p>Description: Electoral Stakeholders on how information pollution has impacted elections, based on their practical experiences and different perspectives.</p> <p>Moderator: Niamh Hanafin, <i>Senior Advisor Information Integrity - UNDP</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Dr Emad al-Sayah, <i>Chairman - High National Election Commission (HNEC), Libya</i> B. Christian Cirhigiri, <i>Policy Officer - Digital Peace, Search for Common Ground (SfCG)</i> C. Patient Ligodi, <i>Journalist - Actualite.cd</i> D. Vusumuzi Sifile, <i>Executive Director - Panos, Zambia</i>
13:00 - 14:30	Lunch
14.30 - 15.30	<p>Session 5: Identifying and Responding to Electoral Information Pollution</p> <p>Description: How electoral information pollution is defined, can be accurately identified and what contributes to effective responses.</p> <p>Moderator: Darren Nance, <i>Chief Electoral Officer - UNMISS South Sudan</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Lutz Guellner, <i>Head of Strategic Communications (Foreign Information Manipulation and Interference) - European Union</i> B. Lara Levet, <i>Policy Officer - Meta</i> C. Qadaruddin Shishir, <i>Editor - AFP Fact-Check Bangladesh</i> D. Ransford Wright, <i>National Coordinator - Independent Radio Network (IRN) Sierra Leone</i>
15.30 - 16.30	<p>Session 6: Building Public Resilience to Information Pollution</p> <p>Description: How societies and the broader information ecosystem can be strengthened to support the public in being less susceptible to election information pollution</p> <p>Moderator: James Deane, <i>Co-founder - International Fund for Public Interest Media</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Kelvin Aguirre, <i>Commissioner, - Consejo Nacional Electoral (CNE), Honduras</i> B. Adeline Hulin, <i>Project Coordinator - UNESCO</i> A. Jad Hani, <i>Media Researcher - Samir Kassir Foundation</i> B. Alasdair Stuart, <i>Advisor/ Research Manager - BBC Media Action</i>
16:30 - 17.00	Coffee Break
17.00 - 18.00	<p>Session 7: Approaches to Regulating Political Speech and Information Pollution during Elections</p> <p>Description: To consider the most effective ways of regulating online political speech around an election to ensure a level playing field, protect freedom of expression, prevent hate speech and incitement to violence.</p> <p>Moderator: Guilherme Canela, <i>Chief Freedom of Expression and Safety of Journalists Section - UNESCO</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Sherri Aldis, <i>Director - UN Regional Information Centre for Western Europe</i> B. Akaki Beridze, <i>Legal Maintenance Division - Central Election Commission of Georgia</i> C. Victor Bwire, <i>Deputy CEO - Media Council of Kenya</i> D. Krisztina Stump, <i>Head of Unit, Media Convergence and Social Media - DG CNECT, European Commission</i>

DAY 2

CHALLENGES AND OPPORTUNITIES TO BUILDING INCLUSIVE ELECTIONS

9.00 - 10.00	<p>Session 8: Global Trends on the Impact of Programming around Peaceful and Inclusive Elections</p> <p>Description: What inclusion looks like in the election process and how it can be achieved</p> <p>Moderator: Aleida Ferreya, <i>Global Lead on Democratic Institutions - UNDP</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Asha Allen, <i>Advocacy Director for Europe - Center for Democracy and Technology (CDT)</i> B. Keare Castaldo, <i>Election Adviser - OSCE Office for Democratic Institutions and Human Rights (ODIHR)</i> C. Lluís Rodriguez, <i>Expert on Inclusion - UNDP</i> D. Lenka Homolkova, <i>CTA - UNDP Liberia</i>
10.00 - 10.30	Coffee Break
10.30 - 11.30	<p>Session 9: Successes and Failures in designing Gender- Inclusive Electoral Processes: Country Experiences</p> <p>Description: Country experiences in building inclusivity within elections and broader democratic processes, focusing on gender.</p> <p>Moderator: Najia Hashemee, <i>Regional Elections Advisor Arab States - UNDP</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Ariunzaya Ayush, <i>Secretary - Mongolian People's Party</i> B. Yuliya Shypilova, <i>Programme Officer - INT IDEA</i> C. Takawira Musavenga, <i>- UNDP, CTA Zambia</i> D. Bizuwork Ketete, <i>Board Member - NEBE</i>
11.30 - 12.10	<p>Session 10: Sustaining Peace during Electoral Processes: Programmatic Guidance from SELECT</p> <p>Description: An exchange on the SELECT research streams, and the key learnings.</p> <p>Moderator: Sebastien Coquoz, <i>Conflict Prevention and Elections Policy Officer - EEAS</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Saré Knoope, <i>Project Manager SELECT - UNDP</i> B. Zana Idrizi, <i>Lead Expert Inclusive Governance Workstream - UNDP</i> C. Ajay Patel, <i>Lead Expert Information Integrity Workstream - UNDP</i> D. Brinda Gangopadhyia Lundmark, <i>Lead Expert Gender Workstream - UNDP</i>
12.10 - 12.30	<p>Session 11: Digital Threats to Inclusion</p> <p>Description: A presentation to take a wide angle on how digital threats can threaten modern election processes</p> <p>Moderator: Emanuele Sapienza, <i>Global Lead - Civic Space - UNDP</i></p> <p>Speaker: Deborah Brown, <i>Senior Researcher - Human Rights Watch</i></p>
12.30 - 14.15	Lunch
14.15 - 14.45	<p>Session 12: Causes and Consequences of Electoral Violence</p> <p>Description: How election violence is used by electoral stakeholders and the role on information pollution in fomenting it.</p> <p>Moderator: Panto Letic, <i>Chief Electoral Advisor - UNDP Libya</i></p> <p>Speaker: Professor Ursula Daxecker, <i>Principal Investigator - EVaP</i></p>
14.45 - 15.45	<p>Session 13: Addressing Online and Offline violence against Women in Public Life</p> <p>Description: A discussion to focus on the different forms of political violence against women - and other marginalised communities - in public life, exploring strategies and programs that can be deployed to combat the concern.</p> <p>Moderator: Luis Martinez-Betanzos, <i>Senior Electoral Advisor, Latin America - UNDP</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Diana Atamaint, <i>President - Consejo Nacional Electoral del Ecuador</i> B. Santiago Aroa, <i>Gender Specialist - UNDP</i> C. Maria Belen Luna Sanz, <i>- HateAid</i> D. Alvaro Beltran Urrutia, <i>- UNDP Peru</i>
15:45 - 16.00	Coffee Break
16.00 - 17.00	<p>Session 14: Youth-Inclusive Digital Technology to foster Peaceful and Inclusive Elections</p> <p>Description: How technology can increase the inclusivity of elections, as well considerations and safeguards needed.</p> <p>Moderator: Micky Elanga, <i>Digital Inclusion Expert, EU Digital for Development Hub - European Commission</i></p> <p>Speakers:</p> <ul style="list-style-type: none"> A. Pauline Deneufbourg, <i>Youth Advisor - UNDP</i> B. Wani Geoffrey, <i>Youth Leader, Software Engineer - AlertMe</i> C. Kayle Giroud, <i>Associate Director - Global Cyber Alliance</i>

DAY 3



FUTURE OF ELECTIONS		
9.00 - 10.00	Session 15: Description: Moderator: Speakers:	Practical Approaches to Enhance Electoral Inclusion and Integrity A discussion to highlight the work of UNDP in the development of approaches, technology and programmatic approaches, focusing on the various information integrity tools, other resources, and the opportunity to introduce other initiatives. The session should focus on how to design approaches and then introduce tools – by types of activity. Niamh Hanafin , <i>Senior Advisor Information Integrity - UNDP</i> A. Alpha Senkpeni , - <i>Local Voices, Liberia</i> B. Osama Aljaber , <i>Digital Democracy Specialist - UNDP</i> C. Gabriel van Oppen Ardanaz , <i>Electoral Assistance Programme Specialist - UNDP</i>
10.15 - 11.45	Session 16: Description: Moderator: Speakers:	Future Elections: How Technology and Innovations will Shape Elections A discussion on how the work of election administrators will be affected by future developments in digitisation and technology Skye Christensen , <i>Chief Technical Advisor - UNDP</i> A. Dr. Hab. David Dueñas-Cid , - <i>Gdansk University of Technology, Poland</i> B. Janet Love , <i>Vice Chair - Electoral Commission of South Africa</i> C. Dr. Piero Alessandro Corvetto Salinas , <i>Chief - National Office of Electoral Processes (EMB), Peru</i> D. Sonia Bea L. Wee-Lozada , <i>Director - Office for Overseas Voting (OCV), Commission on Elections, Philippines</i> E. Elliott Wilkes , <i>Cybersecurity Expert, - CTO, ACDS, UK Gov</i> F. Mrs. Shaildabekova Karmabekovna , <i>Chair - CEC, Kyrgyzstan</i>
11.45 - 12.00		Coffee Break
12.00 - 12.30	Session 17: Speakers:	Closing A. Sarah Lister , <i>Head of Governance - UNDP</i> B. Petr Jelinek , <i>Deputy Head of Unit - FPI</i> C. Georges van Montfort , <i>Deputy Director - UNDP Brussels</i>



SELECT

Information integrity topic:

https://www.sustainingpeace-select.org/the-knowledge-hub/?_sft_category=information-integrity

Youth Participation topic:

https://www.sustainingpeace-select.org/the-knowledge-hub?_sft_category=youth-participation

Knowledge hub:

<https://www.sustainingpeace-select.org/>

X (twitter): @UNDP_SELECT

Email: select.tools@undp.org

