Community of Democracies

Impact of Technology on the Future of Democracy

Trend and Policy Brief

July 2024

Community of Democracies – Working Group on Democracy & Technology (WGD&T)

Community of Democracies

Introduction

The next generation of technology is approaching rapidly. This next wave of technology trends will usher in improved ways for people to interact with each other, gain access to valuable services, and participate in democratic processes. However, these trends also present the potential for new vulnerabilities, methods of exploitation by individual, organized, or nation-state actors, and risks to the people that utilize these new technologies in the digital ecosystem.

In addition, there remains a level of uncertainty regarding the effects these trends will have on the future of democracy. Despite these potential unknowns, it is imperative that governments continue to build on their efforts to design, develop, and implement policies to govern and regulate these trends. This brief is an attempt to provide lawmakers, policymakers, and implementers with recommendations based on the most relevant technologies and associated trends based on the expertise and knowledge of the WGD&T.

The tenets of the policies in this brief leverage the core democratic principles and practices outlined in the Warsaw Declaration[1].

This brief complements the Community of Democracies' work and mission. Understanding the trends and designing recommendations to address them provide the necessary context as well as the stakes toward a roadmap to help the coalition to contribute to strengthening democratic governance in the new digital age as well as combating the misuse of these technologies. The brief will also contribute towards the Community of Democracies and its partners' efforts toward the implementation of the 2030 Agenda for Sustainable Development as the greater understanding of the following technology trends are critical as they affect most of the 17 Sustainable Development Goals (SDGs).

[1] The Warsaw Declaration is the founding document of the Community of Democracies. It sets out 19 principles of human rights, democracy, and the rule of law for the effective establishment and consolidation of democracy: https://community-democracies.org/app/uploads/2016/10/2000-Warsaw-Declaration-ENG.pdf

Community of Democracies

Definitions

The terms in this section are present throughout the rest of the brief. The definitions were developed based on a collaboration between the members of the WGD&T combined with open-source official definitions from the United Nations, Cybersecurity and Infrastructure Security Agency (CISA), The European Union (EU), and the International Telecommunication Union (ITU). These definitions are meant to provide additional context within the trends and policy recommendations in the subsequent section.

- **Security –** Protection of human rights – civil, cultural, economic, political, and social.
- **Cybersecurity –** Collection of tools, policies, concepts, safeguards, guidelines, actions, training, assurance, and technologies utilized to protect the digital ecosystem, organisations, and user assets.
- **Information Integrity** – Refers to the accuracy, consistency, and reliability of information.
- **Critical Infrastructure (CI)** – Refers to election systems as a part of a country's infrastructure, but also other areas of critical national infrastructure (CNI) such as water, electricity, transportation, finances, etc. Digital Public Infrastructure (DPI) – Encompasses the tools and systems required to make digital life function. This includes the wiring of the Internet, institutions such as Domain Name System (DNS), and the software that keeps the Internet running.

Community of Democracies

Themes

There are several themes that appear in the trends and recommended policies in this brief. The themes are important for understanding the trends and recommendations in service of the protection of democratic ideals, processes, and principles as these trends become more widespread in the digital ecosystem. The themes listed here are important to call out in the new and ever-changing digital ecosystem. They represent some of the principal areas that are imperative to consider in ensuring proper governance and understanding of the emerging trends and policy recommendations listed in the subsequent section.

- **Agency –** The capacity of an actor (e.g., government, organisation, citizen) to make decisions and implement actions within the digital environment.
- **Accountability –** Refers to the responsibility, scrutiny, and oversight required to ensure that new technologies and trends are not abused by government or commercial entities that could jeopardize the rights of citizens in the digital ecosystem.
- **Ethics -** Organisational and social norms established and accepted nationwide that govern how people and communities behave in the digital ecosystem. This includes how technologies are designed, implemented, and utilised by stakeholders across the ecosystem.
- **Inclusivity –** Effective service and engagement of all people in the digital ecosystem; ensures that policies, laws, processes, and services are accessible and responsive to all members of a society, including an intersectional perspective regarding online gender-based violence and its effects on women in the digital ecosystem.
- **Pervasiveness –** Across the following trends, emerging technologies play a significant role in their effect on democratic processes and citizen wellbeing. These emerging technologies include Generative Artificial Intelligence (AI), Augmented Reality, Virtual Reality, Quantum Computing, the Internet of Things (IoT), and cloud-based technologies. All of which require government regulations, frameworks, and policies with stipulations based on the trends and recommendations in the following sections.
- **Reliability –** Refers to the accuracy and dependability of the software, hardware, and other related systems that make up the digital ecosystem, related technologies, and services that these provide – or inhibit.
- **Resilience –** Persistence of democratic practices in the digital ecosystem to continue without any sustained decline and to avoid any part of it becoming undemocratic.
- **Transparency –** Refers to the openness and access to information and processes in the digital ecosystem and related technologies that enable – or inhibit at times.

Community of Democracies

Methodology

For this Trend and Policy Brief, the WGD&T used a qualitative approach in the methodology to help combine certain initial trends and down-select others to identify and prioritize five (5) trends to discuss and to develop policy recommendations for in the subsequent sections. A more quantitative and detailed analysis will follow this initial brief in the future.

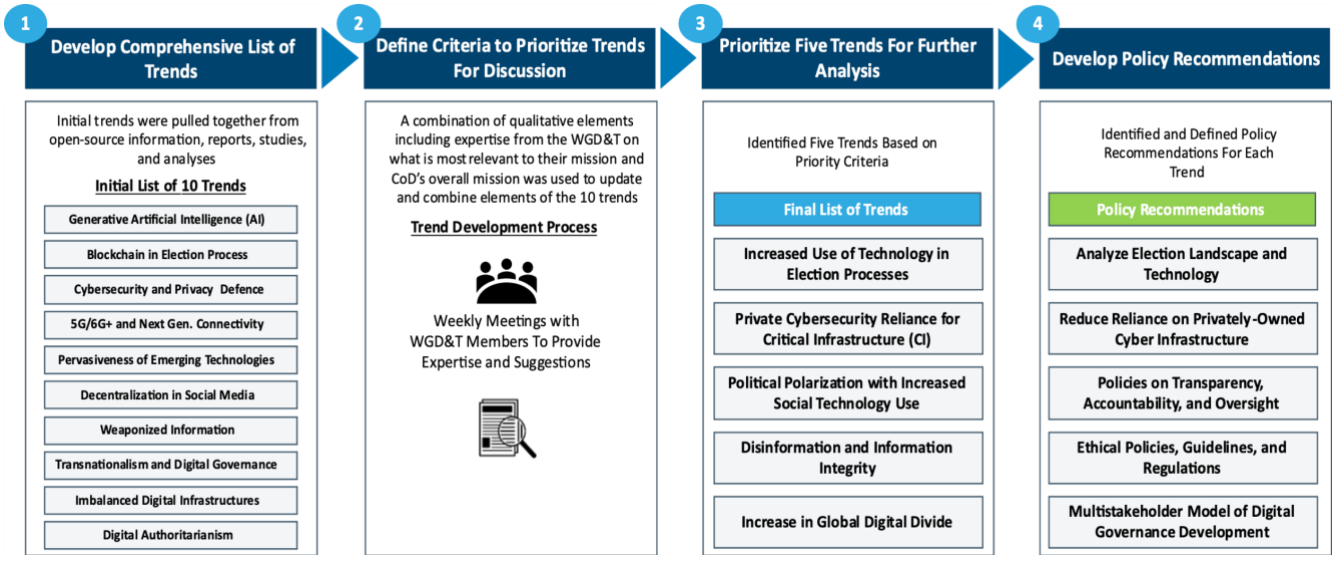

Figure 1: WGD&T Methodology on Foresight Trends and Recommendations

Community of Democracies

Trends and Policy Recommendations

This brief identifies five (5) trends that have the potential to affect the state of democracy in the coming years. Based on these trends, there are five (5) corresponding policy recommendations that can help address these trends, by bolstering the improvements these technologies provide, regulating the technologies and the organisations that manage them, and by mitigating the threats that arise from these technologies in the digital ecosystem.

Each trend is broken down by its overall definition and its impact on democracy. Following this, the corresponding policy is provided, broken down by its definition and rationale to address the trend.

1A. Trend: Increasing Use of Technology for Election Process

- **Definition:** This encapsulates the use of electronic systems and software to support the distinct stages of the election process, among them, voter and candidate registration; casting, counting, and tabulation of votes; election result management and reporting; development of electoral databases; and reporting and oversight of political finance. These systems could range from software-enabled online voting platforms to hardware-enabled electronic voting machines at polling places. This trend overlaps with trend 2A, which considers the importance of cybersecurity and its role in the protection of critical infrastructure (CI), particularly regarding election systems.
- **Impact:** The use of technology in elections can enhance the efficiency and transparency of election institutions; it especially affects the processes related to election administration, management of voters databases, information systems, result transmission and reporting, and traceability mechanisms for all the steps of the electoral process. It can also improve the quality of public services and provide voters, candidates, and other participants in the electoral process with the possibility to engage with key components of the electoral framework easily and swiftly. It can also enfranchise citizens who may lack the means or capacity to travel to the polling places and thus allow for more participation in elections by citizens including young people, those with reduced mobility, women, rural populations, and other marginalized groups, who otherwise would not engage in the democratic process. The use of technology can reduce the financial and time resources required for certain electoral operations. Moreover, electronic platforms have the potential to serve as efficient instruments for bolstering the capabilities of electoral administration and offering enhanced training support. Furthermore, they can be extensively utilised for educating and informing the broader public to promote a greater level of transparency. However, this reliance on technology also raises concerns due to the inherent risks related to security or a low level of understanding of the technical process, which could lead to diminishing trust in electoral processes, provide fertile ground for the spread of disinformation,

and open up opportunities for individual, organized, or nation-state actors to manipulate the votes, exploit the democratic process, or prevent it overall. Increased reliance on technology for voting may also disenfranchise voters in places where entire populations, or specific, marginalized communities, are unconnected and/or lack knowledge of how to use Internet infrastructure.

1B. Recommendation: Analyze Election Landscape and Technology

- **Definition:** Governments should develop detailed analyses addressing trust, transparency, and accountability in electoral processes and democratic institutions. Efforts should be taken to understand the electoral, political, and social landscape and technology *may* be considered as one potential solution to bolster trust, transparency, and accountability. Before any technology is introduced, the technical, ethical, legal, and social factors that would have an effect on elections – both in-person and electronically – should be analyzed. Additionally, conducting ex ante awareness-raising campaigns with recommendations will be beneficial and judicious before fully employing any new technology. This would include the baseline of a rigorous compliance process for any companies that provide the software and/or hardware that is used in voting processes. This analysis can build on previous studies that have explored the impact of technologies on the election process.[2][3] The results of this analysis and compliance baseline will be shared with a multistakeholder group to help promote a more legitimate, transparent, and trusted electoral process with comprehensive oversight on the software and hardware that would be used in every phase of the process.
- **Rationale:** Before proper policy can be enacted governments, with the help of a multistakeholder group, conduct a more thorough analysis of the global election landscape – with a focus on any technology being utilised that may have affected the democratic process. This analysis will be necessary on a periodic basis to ensure any vulnerabilities or gaps are addressed before, during, and after any policies can be developed and implemented by governments (national, regional, or local). These analyses provide an overview of the transparency, ethical integrity, accountability, trust, and overall fairness of these systems as well as how the increasing pervasiveness of emerging technologies may affect the systems and processes.

2A. Trend: Reliance on Private Cybersecurity for Critical Infrastructure

- **Definition:** As the digital ecosystem grows, so does the need for increased protection of cybersecurity that protects the critical infrastructure that is a main foundation of this ecosystem. The cyber protection of this critical infrastructure is often owned by private entities or at least monitored by them. In the instance of election software in the United States for example, 90

[2] Trasys International, "Study on the Impact of New Technologies on Free and Fair Elections," 2021: https://commission.europa.eu/system/files/2022-12/Annex%20III_Explored_use_cases_20210319_dsj_v2.0_clean_PUBLIC.pdf

[3] "Technology in Elections – Best Practices in Using Digital Tools and Platforms in the Community of Democracies": https://community-democracies.org/app/uploads/2022/09/Report-Technology-in-Elections.pdf

percent is owned by three private companies.[4] There is minimal oversight of these private companies that own the software and hardware. There is an increased need for cybersecurity software, hardware, and most importantly, personnel, but this need is being met without proper oversight, accountability, and vetting. The majority of these protections have been – and continues to be – provided by private and commercial entities rather than government organisations.

- **Impact:** The level of investment in cybersecurity for critical infrastructure and personnel will determine the level of vulnerability across areas such as healthcare, banking, education, and government. A lack of sufficient cybersecurity opens up these areas to state and non-state actors who may be able to sabotage systems or take them offline. A lack of cyber resilience embedded in the overall cybersecurity of infrastructure can worsen the impact of a successful attack. This could strain government budgets as they will require a constant investment in the private sector to protect the underlying systems that ensure citizen services across a range of industries. In addition, a reliance on private entities that own critical digital infrastructure can be dangerous in times of conflict (e.g., Starlink in Ukraine in 2023). The lack of oversight and proper vetting of vendors means governments cannot provide adequate transparency or accountability of what is being used to protect critical systems and infrastructure.

2B. Recommendation: Reduce Reliance on Privately-Owned Cyber Infrastructure

- **Definition:** Government agencies need to expand their own cybersecurity and capacity and should explore whether increased investment in Digital Public Infrastructure (DPI) can be used effectively to bolster democratic and civic participation. Additionally, governments design, develop, and implement an updated set of regulations (and updated regulatory frameworks), policies, and standards to govern the underlying cyber infrastructure that has become essential to provide citizen services and connections. Clearly defining digital infrastructure obligations and security standards promotes a level of transparency, corporate accountability, and government reliability.
- **Rationale:** Beyond fostering DPI, developing a legal framework, licensing rules, data governance policies, and cybersecurity regulations are necessary to prevent private companies from taking unilateral decisions that could affect the wellbeing of citizens and democratic processes. Building out these policies, updating frameworks, and strengthening governance rules gives national entities more independence in supporting the needs of citizens without having to rely on private entities for major interventions or support at critical times (e.g., cyber-attack that brings down a network), and thus gives these entities a stronger level of resilience within their digital networks.

3A. Trend: Political Polarization Through Increased Social Technology Use

- **Definition:** The use of technology to communicate, transact, and provide services has increased year-over-year for the past several decades. Notably**,** social media use across the globe has

[4] The Brennan Center, "A Framework For Election Vendor Oversight," 2019: https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight

increased by eight percent in the last year – from 4.72 billion users in January 2023 to 5.04 billion[5] in January 2024. This social media use, particularly in the weeks/months before, during, and immediately after an election, has deepened political polarization.

Information has become segmented, opinions are siloed and rendered more extreme through online echo chambers, and inflammatory and violent content runs rampant – often perpetrated by bots[6] – on various online platforms.

- **Impact:** The algorithms of these technology platforms have only further increased political polarization. The organisations that own these technology platforms have continued to be unaccountable and opaque, despite the ethical dilemma that has arisen from these technology sources. It has decreased healthy democratic discourse, elevated far-right and far-left wing language, and promoted violent and manipulative content. In addition, it has caused the participation of marginalized groups – including women – to decline. The decline of public trust in government and media due to the abuse of these technologies has led to further erosion of the democratic process. The pervasiveness and increasing use of artificial intelligence (AI) and other emerging technologies have – and will continue – to exacerbate this political polarization without proper regulatory and accountable guardrails from governments and civil society organisations.

3B. <u>Recommendation:</u> Promote Policies on Algorithmic Transparency, Social Media Accountability, and Oversight of Commercial Technology

- **Definition:** Laws, policies, and guidelines require technology platforms that are citizen-facing (i.e., that citizens use on a day-to-day basis) to be transparent and publish details on their algorithms and metrics to an open-source environment. In addition, create playbooks and simple training documents for citizens and organisations to understand how these technology platforms and algorithms work as well as list several potential implications of these algorithms. These potential implications could be developed in a multistakeholder setting between the owners of algorithms and select government and civil society leaders knowledgeable of potential effects.
- **Rationale:** This ensures a higher level of transparency to governments and citizens on the technology platforms – as well as the algorithms – they are using. It also creates accountability for the owners of these platforms from both a regulatory perspective but also accountability to the users of the technology platform. Developing additional oversight mechanisms on commercial technology firms whose software and/or hardware is used by governments and citizens is important to ensure they design, develop, and implement new technologies based on applicable and ethical laws, policies, and guidelines that have been passed or published.

---

[5] Global Web Index, "Social Media Usage & Growth," 2024: https://www.gwi.com/reports/social

[6] PNAS Research, "Bots Increase Exposure to Negative and Inflammatory Content," 2018: https://www.pnas.org/doi/full/10.1073/pnas.1803470115

Community of Democracies

4A. Trend: Rise of Dis- and Misinformation

- **Definition:** Increasing amounts of mis- and disinformation are undermining trust and information integrity. The sophistication and ubiquity of disinformation is growing through the use of generative AI. Authoritarian governments are co-opting disinformation to discredit opposition and bolster their own authoritarian messages. A lack of digital literacy means that misinformation and disinformation will continue to be a serious challenge for governments and average citizens utilizing online services and platforms.
- **Impact: I**nformation is increasingly being weaponized by oppressive governments to undermine trust in democratic institutions and processes. Recent studies[7] have shown the detrimental effect of disinformation, particularly around discouraging women and other marginalized groups from participating in the electoral process. Personal data that is collected, transmitted, and stored by companies can potentially be sold to individual, organized, or nation-state actors to support more realistic and targeted disinformation campaigns to sow dissent and enable repression and illegal surveillance.

4B. Recommendation: Develop Ethical Policies, Guidelines, and Regulations on Information Integrity and Governance While Promoting Digital Literacy

- **Definition:** Articulate an affirmative vision of information integrity; invest in independent, trustworthy media; support civic resilience through digital and media literacy efforts; support content provenance and labelling requirements. Develop and implement clear guidelines, codes of conduct and codes of practice regulating the activity of very online platforms and very big search engines. Content authenticity laws and/or policies should include strict ethical guidelines on content provenance, particularly with regard to the use of generative AI and other data manipulation technologies. It would be prudent to reference the White House's Roadmap on Integrity Research and Development[8] to help develop these guidelines and potential laws as well as organisations (e.g., C2PA) that can advise on content provenance and digital watermarking to develop these guidelines, laws, and policies. Additionally, create training materials to inform citizens on how to spot mis and/or disinformation (these training materials may overlap with Recommendation 3B). Fostering digital and media literacy skills should be included in the school curriculum from the earliest stages of education.
- **Rationale:** Governments, businesses, and other stakeholders should collaborate to develop and implement these ethical guidelines to help combat and mitigate the prevalence of misinformation and, in turn, its use by authoritarians as disinformation in the continued increase of weaponization of data across the digital landscape. Finally, creating a multistakeholder group that promotes investing in training materials that are accessible, can raise the level of digital literacy

[7] EU Disinfo Lab, "Gender-Based Disinformation: Advancing Our Understanding and Response," 2021: https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response/

[8] National Science & Technology Council, "Roadmap for Researchers on Priorities Related to Information Integrity Research and Development," December 2022: https://www.whitehouse.gov/wp-content/uploads/2022/12/Roadmap-Information-Integrity-RD-2022.pdf

in areas and marginalized populations (e.g., women, low socioeconomic groups) where it is lacking.[9]

5A. Trend: Increase in the Global Digital Divide

- **Definition:** The coming decades will see migrations across different geographies as well as an increase in globalization of commercial enterprises and supply chains. While some countries have experienced a massive increase in the expansiveness and sophistication of their underlying digital infrastructures, much of the world has had limited to no increase in their infrastructures, thus further exacerbating the digital divide.[10] While some countries have rapidly grown their Digital Public Infrastructure, many marginalized communities remain unconnected and unable to access an increasing number of government services that are provided online.
- **Impact:** Frameworks for digital governance may not be able to keep up with the changes in those using the technology, especially with fragmented digital laws and regulations based on regions or countries rather than international standards. An imbalance in these infrastructures and a lack of interoperability further increases the digital divide between the rich and the poor as even when the poor gain access to the Internet, they remain vulnerable and far behind the speed, strength, and understanding of digital and cybersecurity. Siloing of information may result and further exacerbate the divide, causing more harmful impacts on minorities including women, those with a lower socioeconomic background, and marginalized populations.

5B. Recommendation: Implement a Multistakeholder Model of Digital Governance Development

- **Definition:** Commit to and uphold multistakeholder model of Internet governance that emphasizes participation between governments, private companies, and civil society organisations. This framework (or frameworks) establishes the accountability, roles, decision-making, and change management authority (when new, emerging technologies or platforms are implemented) for these stakeholders.
- **Rationale:** This level of multistakeholder cooperation will play a crucial role in digital ecosystem dialogues. This may be seen as a promulgation of public-private partnerships, which by enhancing its format in digital governance will be important in future decision-making processes. It ensures no entities are left out of the decision-making process – particularly the younger generations that use the Internet at a higher percentage – to instill human rights and freedoms in technology development, governance, and implementation of technologies into areas that affect people across genders, cultures, socioeconomic backgrounds, countries, regions, and the world. This will ensure that everyone in the digital ecosystem collaborates as the pervasiveness of emerging technologies continues to affect the development of digital governance rules and norms.

---

[9] Read, Alex, A Democratic Approach to Global AI Safety, Westminster Foundation for Democracy, 2023: https://www.wfd.org/what-we-do/resources/democratic-approach-global-ai-safety

[10] United Nations, "Widening Digital Gap between Developed, Developing States Threatening to Exclude World's Poorest from Next Industrial Revolution, Speakers Tell Second Committee" United Nations Press, October 2023: https://press.un.org/en/2023/gaef3587.doc.htm

Community of Democracies

Sources

1. Community of Democracies, “Warsaw Declaration toward a Community of Democracies,” June 2000: https://community-democracies.org/app/uploads/2016/10/2000-Warsaw-Declaration-ENG.pdf
2. Trasys International, “Study on the Impact of New Technologies on Free and Fair Elections,” 2021: https://commission.europa.eu/system/files/2022-12/Annex%20III_Explored_use_cases_20210319_dsj_v2.0_clean_PUBLIC.pdf
3. Community of Democracies, “Technology in Elections – Best Practices in Using Digital Tools and Platforms in the Community of Democracies”: https://community-democracies.org/app/uploads/2022/09/Report-Technology-in-Elections.pdf
4. The Brennan Center, “A Framework For Election Vendor Oversight,” 2019: https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight
5. Global Web Index, “Social Media Usage & Growth,” 2024: https://www.gwi.com/reports/social
6. PNAS Research, “Bots Increase Exposure to Negative and Inflammatory Content,” 2018: https://www.pnas.org/doi/full/10.1073/pnas.1803470115
7. EU Disinfo Lab, “Gender-Based Disinformation: Advancing Our Understanding and Response,” 2021: https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response/
8. National Science & Technology Council, “Roadmap for Researchers on Priorities Related to Information Integrity Research and Development,” December 2022: https://www.whitehouse.gov/wp-content/uploads/2022/12/Roadmap-Information-Integrity-RD-2022.pdf
9. Read, Alex, A Democratic Approach to Global AI Safety, Westminster Foundation for Democracy, 2023: https://www.wfd.org/what-we-do/resources/democratic-approach-global-ai-safety
10. United Nations, “Widening Digital Gap between Developed, Developing States…,” United Nations Press, October 2023: https://press.un.org/en/2023/gaef3587.doc.htm