IRIS
Information Resilience
& Integrity Symposium

RESEARCH PAPER

Beyond Electoral Moments: GenAI, Information Integrity, and the Future of Democratic Resilience in Asia-Pacific

PANEL 4 | The Role of Information in Democratic Resilience

Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Universitas Gadjah Mada
Fakultas Ilmu Sosial dan Ilmu Politik

Center for Digital Society

Dr. Abdul Gaffar Karim

Dr. Abdul Gaffar Karim is Head of the Department of Politics and Government at Universitas Gadjah Mada, where he leads research and education in democracy, civil society, and electoral politics. He also directs PARES Indonesia and coordinates Election Corner (EC) and Collaborative Hub for Politics and Policy on Sustainability (CoPPS). His work spans political risk analysis, democratic governance, and policy consulting, with recent projects on environmental democracy, human rights education, and Indonesia's new capital (IKN Nusantara) development.

This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.

Beyond Electoral Moments: GenAI, Information Integrity, and the Future of Democratic Resilience in Asia-Pacific

Dr. Abdul Gaffar Karim

This paper explores how Generative AI (GenAI) is accelerating the erosion of democratic resilience in the Asia-Pacific region. Moving beyond electoral moments, it argues that democracy is being undermined through systemic information manipulation—affecting public cognition, institutional credibility, and civic space. Drawing on works by Applebaum, Levitsky & Way, and Gamboa, the paper synthesizes conceptual insights with regional case studies to show how GenAI transforms disinformation into a tool of autocratization. It proposes a multi-stakeholder architecture of information resilience centered on empowered civil society, adaptive regulation, and regional collaboration. The paper concludes that safeguarding democracy in the GenAI era requires not only technological solutions but also a collective commitment to rebuilding trust, truth, and transparency in the public sphere.

Keywords: generative AI, democratic resilience, information integrity, civil society

Democracy Amidst Information and GenAI Storm

In 2024, several countries in Asia and the Pacific held general elections. Taiwan held its presidential election in January, the same month as the legislative election in Bangladesh. In February, there were legislative elections in Pakistan and Indonesia, while throughout April, May and June there were a series of general elections in India, South Korea, the Solomon Islands, and several other countries. Towards the end of the year, Japan held its legislative election in October, and Indonesia its presidential election in November. With a wide range of voter turnout (VTO) (ranging from 54% in Japan to 82% in Indonesia), 2024 was a "super election year" for Asia-Pacific, with more than a billion citizens participating in national and local elections. The largest number of voters was in India with more than 600 million voters, followed by Indonesia with more than 167 million voters. This data is easily available through Google.

With a quick Google search, one can also learn that Asia-Pacific countries like India, Indonesia, South Korea, Pakistan, and Taiwan are facing serious challenges related to the use of generative AI in the electoral process. This technology is used to create fake content that influences public opinion and the integrity of democracy. It was all over the news that the 2024 super-elections in Asia-Pacific witnessed the misconducts of GenAI, from deepfake content (such as the use of AI-generated videos to impersonate or misrepresent political figures) to disinformation campaigns (including coordinated use of AI to spread false or misleading narratives). The 2024 elections in Asia-Pacific showed that GenAI is not only changing the way campaigns and votes are conducted, but also eroding the fundamental foundations of everyday democracy—from freedom of expression to government accountability.

How serious is this issue? I want to discuss this from the perspective of information manipulation. In politics, information manipulation is, of course, not a recent development. But thanks to three significant changes, GenAI has turned it into a weapon of mass destruction for democracy. The first is the extent of the production of misinformation, which has now grown to an industrial level. For instance, according to OpenAI, 100 million people create synthetic content every day. Second, information that is too realistic, like the deepfakes of the 2024 Indian elections, is eroding public confidence in democratic systems.

The third change is the automation of cross-border cyberattacks, as demonstrated by geopolitical players' attempts to undermine the legitimacy of the 2024 Taiwanese elections.[1]

This problem is existential because if we refer to Habermas's opinion, democracy rests on a rational public sphere.[2] And that is the challenge: the rational sphere is shrinking due to erosion by a flood of synthetic content that erodes society's collective ability to distinguish fact from fiction. When the war on truth becomes a war on democracy itself, the last line of defense is not technology, but the reconstruction of the collective infrastructure of trust.

Scope and Theoretical Framework

This paper analyzes the mechanism of democracy degradation by GenAI, then unravels the dilemma of stakeholder coordination, extracts lessons from the Asia-Pacific response, and formulates evidence-based policy recommendations. The ultimate goal is not only to answer today's panel question, but also to advance a collective agenda: information integrity must be the breath of democracy, not just a shield during elections.

At this point, I must emphasize that the use of GenAI in politics is still relatively news. Many AI tools used in political activities are still in the development stage and have only become widely used in the last couple of years. The use of deepfake videos, synthetic voices, and political chatbots has only really expanded in recent times. A 2024 report by the Carnegie Endowment stated that the impact of GenAI in politics is indeed increasing, but it remains tentative and contextual.[3] This paper attempts to balance such “academic doubts” with the vast reportage on fake news in the 2024 Asia-Pacific elections.

However, this paper is not intended to be a comprehensive empirical study of the impact of GenAI. Rather, it is more a conceptual study that synthesizes critical perspectives from some leading works in the study of democratic decline, to answer the fundamental question: *How can information integrity become the backbone of democratic resilience in the GenAI era?*

The analysis presented here is reflective, not new research. This is important to emphasize, especially considering that GenAI is a growing phenomenon, even though the signs of its negative impacts are starting to become worrying. The focus of this paper is on linking four

[1] Microsoft Threat Intelligence. (2023). *Microsoft Digital Defense Report: Building and improving cyber resilience*, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
[2] Jurgen Habermas. (1989). The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. MIT Press. (Original work published 1962)
[3] R. Csernatoni. (2024). Can Democracy Survive the Disruptive Power of AI? Carnegie Endowement for International Peace https://carnegieendowement.org/research/2024/12/can-democracy-sruvive-the-disruptive-power-of-ai?lang=en

seminal works on 21st-century democratic decline with the contemporary challenges of GenAI. In addition, this paper also utilizes some of the findings of the research I conducted with Puskapol UI and Yayasan Penabulu in 2024. In this section, I would like to briefly review these works.

Four Seminal Works

First, Anne Applebaum in her two works *Twilight of Democracy*[4] and *Autocracy, Inc.*,[5] shows that information manipulation is the ultimate weapon of modern autocracy. Through GenAI, this weapon evolves into hyper-personalized disinformation that targets social rifts and sophisticated surveillance that suppresses dissensus. A twilight zone is produced by this combination, where the public's faith in democratic institutions is steadily undermined and truth is reduced to instrumental tales. The 2024 Indian election deepfake campaign, which falsified the comments of politicians, and the usage of GenAI-based chatbots by totalitarian regimes to monitor their populace, as in Vietnam and Myanmar, are two examples of this tendency in the Asia-Pacific region.

Second, Steven Levitsky & Lucan A. Way's analysis in an article entitled *Democracy's Surprising Resilience* complements this framework by emphasizing that democratic resilience depends on elite cohesion and civil mobilization.[6] These two pillars are very vulnerable to the onslaught of GenAI synthetic content. The flood of mass-produced false information triggers citizens' cognitive exhaustion and paralyzes awareness-based participation. In Indonesia, for example, AI-based hoaxes after the 2024 election about systemic fraud were deliberately designed to weaken civil society and kill the mobilization of criticism of power.

Third, Laura Gamboa wrote a book that is just as interesting as Applebaum's works above, entitled *Resisting Backsliding*.[7] This book reminds us that democracy only survives if the opposition and civil society can design a collective strategy against information disruption. Here, GenAI becomes the main destroyer through two mechanisms: deepfake attacks that damage the credibility of civil society actors, and information overload that floods

[4] Anne Applebaum. (2020). *Twilight of Democracy: The Seductive Lure of Authoritarianism*. New York: Doubleday.

[5] Anne Applebaum. (2024). *Autocracy, Inc.: The Dictators Who Want to Run the World*. London: Penguin Books Limited.

[6] Steven Levitsky & Lucan A. Way. (2023). Democracy's Surprising Resilience. *Journal of Democracy*, 34(4), 5–20

[7] Laura Gamboa. (2022). Resisting Backsliding: Opposition Strategies against the Erosion of Democracy. Cambridge: Cambridge University Press.

independent verification channels, so that civil society is overwhelmed in distinguishing between facts and manipulation.

By synthesizing the views of the scholars above, I argue that the degradation of democracy by GenAI is systemic, goes beyond the electoral moment, and can only be overcome by making information integrity the core of resilience. For me, the collapse of contemporary democracy begins with epistemic collapse. GenAI has accelerated information manipulation into a weapon of mass autocratization that undermines public trust, triggers pathological polarization, and cripples democratic institutions. Therefore, the resilience of democracy in the Asia-Pacific paradigmatically depends on our ability to build a credible information infrastructure – a multi-stakeholder ecosystem that ensures the flow of political truth.

There are three main claims in this argument. *First,* it has to do with determining the extent of the harm. We can use Applebaum's reasoning to argue that information manipulation is a fundamental process of democratic decay rather than a symptom. The *second* has to do with the prerequisites for democratic resilience. According to the framework developed by Levitsky and Way, democratic institutions will endure if they have access to information that can be independently verified. *Third,* we might provide a solution by applying Gamboa's logic, which holds that the creation of reliable alternative information is necessary for opposition to democratic collapse.

Above all, I would want to emphasize that the Asia-Pacific elections in 2024 are merely symptoms. The ability of GenAI to erode everyday democracy—that is, public involvement, policy discourse, and institutional trust—is the true threat. The ruling class will be the only ones able to access democracy if the information ecosystem is left contaminated.

Research on Civil Society Resilience

In 2024, I worked with PUSKAPOL UI and the Penabulu Foundation to perform a study that sought to assess the state of Indonesia's civic space ecosystem.[8] Civil society organizations (CSOs) that operate in the areas of democracy and human rights, the environment and sustainable development, and the inclusion of marginalized groups are the primary focus of this study. The two underlying assumptions of this study are that civil space serves as a battlefield for conflicts between the government and civil society and that CSOs are resilient due to their local roots and community interests.

[8] Puskapol UI (2024). Analisis Sosial terhadap Kondisi Ekosistem Ruang Sipil dan Kerentanan Masyarakat Sipil di Indonesia. Interim report. Puskapol UI & Yayasan Penabulu.

Through focus group discussions and in-depth interviews, it was discovered that the state's violent, political, and legal constraints have significantly reduced Indonesia's civil space. The primary tools of limitation, made worse by the COVID-19 outbreak, are the Mass Organizations Law and the ITE Law. Vulnerable groups like indigenous peoples, women human rights activists, and workers are more affected by the funding, public perception, and internal fragmentation issues that CSOs confront.

Nonetheless, CSOs show resiliency by using creative tactics including cross-organizational cooperation, people's economy, and crowdfunding. Sustaining sustainability and public trust requires enhancing internal capability, accountability, and transparency.

The Decline of Democracy

Democracy does not only live in electoral moments. It pulsates in the daily lives of citizens—in policy dialogues, public participation, and trust in institutions. However, in the increasingly complex digital era, GenAI has become a new threat to democracy, one that is invisible but very real. This technology, once celebrated as an innovative breakthrough, has now become a reality-production machine capable of turning truth into an algorithmic commodity. In this context, GenAI is not just a tool, but an active actor in the process of democratic degradation.

In *Autocracy, Inc.,* Applebaum describes a world moving toward a democratic twilight zone—a murky space where hyper-personalized disinformation and digital surveillance create an atmosphere of systematic distrust. GenAI amplifies this process by creating seemingly convincing false narratives, preying on social rifts, and weakening people's capacity to distinguish between fact and fiction. In such a space, democracy does not suddenly die, but rather slowly loses its epistemic foundations.

The manipulation of public cognition is one of the primary ways that GenAI threatens democracy. In the essay mentioned above, Levitsky and Way stress that social cohesiveness serves as the primary basis for democratic resilience. However, by using microtargeting techniques that foster hate bubbles, GenAI erodes this foundation. In India, for example, anti-Muslim campaigns spread through WhatsApp use voice cloning technology to imitate the voices of religious leaders, spreading provocative messages that divide society. A report from the Pulitzer Center shows how WhatsApp was systematically used by the BJP to spread provocative messages, including old videos manipulated to stir up anti-Muslim sentiment.[9] In

[9] Srishti Jaswal. Inside the BJP's WhatsApp Machine. *Pulitzer Center*. https://pulitzercenter.org/stories/inside-bjps-whatsapp-machine

addition, reports from Al Jazeera[10] and CNN[11] confirm the use of anti-Muslim rhetoric by PM Modi during the 2024 campaign. In Indonesia, a report from Channel News Asia shows that AI was widely used in the 2024 Indonesian elections, including chatbots that spread manipulative narratives.[12] Meanwhile, CNN reported the use of deepfakes in the Indonesian elections, including a video of Suharto revived for political propaganda, showing a similar trend of visual manipulation.[13]

In addition to undermining social cohesion, GenAI also destroys the credibility of democratic institutions. Institutions such as the General Election Commission (KPU), the Constitutional Court, and independent media are the last bastions of democracy. However, deepfake technology has been used to attack their legitimacy. When institutions are no longer trusted, democratic procedures lose their substantive meaning. As a result, society loses common ground in facts, and policy debates turn into identity wars. Pepinsky notes that Indonesian democracy is declining in quality due to the manipulation of information and the personalization of political narratives, leading to polarization and erosion of public trust.[14]

GenAI also systematically undermines civic space, a vital arena for citizens to check power. Laura Gamboa in Resisting Backsliding warns that without a vigilant civil society, democracy will slowly die. GenAI narrows this space in two ways: first, by creating deepfake content that damages activists' reputations; and second, by flooding information channels with hoaxes that civil society organizations are overwhelmed in verifying. In the Philippines, as reported by the Asia Centre, female journalists were victims of voice changeovers used to create fake content that appeared authentic, damaging their reputations and triggering digital harassment.[15] Civil society organizations in Asia face enormous challenges in verifying the massive and rapid production of fake content by GenAI technology. Fact-checking is no longer sufficient as a primary tool due to the volume and speed of disinformation. A Thomson

[10] Yashraj Sharma, 'Infiltrators': Modi accused of anti-Muslim hate speech amid India election. *Aljazeera*. https://www.aljazeera.com/news/2024/4/22/infiltrators-modi-accused-of-anti-muslim-hate-speech-amid-india-election

[11] Rhea Mogul. India's election campaign turns negative as Modi and ruling party embrace Islamophobic rhetoric. *CNN*. https://edition.cnn.com/2024/05/28/india/india-narendra-modi-hate-speech-analysis-intl-hnk/index.html

[12] https://www.channelnewsasia.com/asia/ai-disinformation-deepfakes-indonesia-elections-4091296; lihat juga Sinta Dewi Rosadi. The Use of AI and Social Media for 'Black Campaign' in the 2024 General Elections in Indonesia: A Review of Indonesian Laws on Black Campaign. *Majority World Initiative Papers*. Yale Law School. https://law.yale.edu/sites/default/files/area/center/isp/documents/mwi-sinta-dewi-rosadi_2024-08-01_re-fin.pdf

[13] https://edition.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl/index.html

[14] Brookings Institution. (2024). Indonesia's election reveals its democratic challenges. Retrieved from https://www.brookings.edu/articles/indonesias-election-reveals-its-democratic-challenges/ Brookings Institution. (2024). Why Indonesia's Democracy Is in Danger. Journal of Democracy. Retrieved from https://www.journalofdemocracy.org/onlineexclusive/why-indonesias-democracy-is-in-danger/

[15] https://asiacentre.org/fact-checking-useful-but-no-longer-primary-tool-against-disinformation/

Foundation study on the 2024 Taiwan election found similar evidence, with AI being used to generate massive amounts of fake audio and video, targeting politicians and policy issues, and placing a heavy burden on verification organizations such as the Taiwan FactCheck Center and IORG.[16]

All of this shows that GenAI has turned everyday democratic life into an information battlefield, where truth is the first casualty. When civil society is busy defending itself from deepfake attacks and floods of disinformation, the authorities have more room to seize freedom. A healthy democracy requires a rational and open public space, but GenAI narrows that space by creating a manipulative alternative reality.

Referring to Applebaum, Levitsky & Way, and Gamboa, I can argue that the degradation of democracy by GenAI is systemic and goes beyond electoral moments. Democracy will not survive if its information ecosystem is polluted. Therefore, the resilience of democracy in the Asia-Pacific depends on our ability to build a credible information infrastructure—a multi-stakeholder ecosystem that ensures the flow of political truth. In this context, information integrity is not only a defense tool, but a primary requirement for the survival of democracy itself.

Stakeholder Collaboration Challenges

Amidst the wave of disruption brought about by GenAI, the democratic landscape in Asia-Pacific faces increasingly complex coordination challenges. GenAI is not only changing the way information is produced and disseminated, but also complicating the relationships between stakeholders in the democratic ecosystem. Governments, civil society, digital platforms, and regulators are now faced with an unprecedented dilemma. Fragmentation of interests and capacity gaps are major obstacles to building inclusive and sustainable information resilience.

One of the most fundamental dilemmas is national jurisdiction versus cross-border threats. GenAI has turned disinformation into a transnational weapon that transcends domestic legal boundaries, while regulations (such as Indonesia's ITE Law) are only able to reach local domains. This creates a space for digital impunity for foreign actors.

The second dilemma is the tension between regulatory reactivity and proactivity. In many Asia-Pacific countries, information regulation still operates in a firefighting logic—acting after the damage has been done. The Electronic Information and Transactions Law (UU ITE)

[16] https://www.thomsonfoundation.org/latest/ai-and-disinformation-in-taiwan-s-2024-election/

in Indonesia, for example, is more often used to crack down on content after disinformation has spread widely, rather than preventing it from the start. My research with Puskapol UI and Yayasan Penabulu shows that 72% of criminal cases under the ITE Law actually entangle activists who criticize public policies, while GenAI-based buzzer accounts that spread hoaxes remain free to roam. This creates a paradox: regulations that should protect democracy have instead become a tool of repression against civil society.

This relates to the third dilemma, namely the tension between security and privacy. Under the pretext of maintaining national stability, many governments in the region have begun to use GenAI for mass surveillance. India launched the Trinetra system, an AI-based surveillance system developed by Staqu Technologies and used by the Uttar Pradesh Police. This system combines facial recognition, voice identification, and criminal gang analysis, and is integrated with a digital database containing more than 900,000 criminal records. Trinetra is used to monitor digital activities including social media and VOIPAI to scan citizens' social media.[17] Meanwhile, Singapore developed a Sense-making & Surveillance system in collaboration with the Police and Immigration to detect threats using advanced AI technology. This system is used for content analysis and identification of potential threats to national security.[18] Does this give citizens a sense of security? Not at all. On the contrary: a report by PrivacyEngine and IAPP shows that 68% of consumers in Asia-Pacific are concerned about the privacy of their data, and that data collected by AI systems is often used for surveillance purposes, including against civil society and the opposition.[19]

Beyond the regulatory dilemma, actor fragmentation also presents coordination issues. Civil freedoms are frequently sacrificed in the name of political stability and security. Profit is the top priority for digital platforms like Meta and Google, and their algorithms magnify anything that is divisive and commercially profitable. In the meantime, civic society faces constant cyberattacks, governmental pressures, and a lack of money. 57% of civil society organizations (CSOs) rely on crowdfunding, which can be blocked, according to my previously mentioned data, and foreign contributors have dropped by 40% since 2020. Moreover, internal fragmentation exacerbates the situation: only 12% of CSOs work together on many topics, and the gap in capability between urban and rural CSOs is growing.

[17] https://cxotoday.com/press-release/staqu-collaborates-with-up-police-to-launch-ai-powered-trinetra-2-0-featuring-new-crime-gpt-feature/

[18] https://www.htx.gov.sg/who-we-are/what-we-do/our-expertise/sense-making-surveillance

[19] https://iapp.org/resources/article/privacy-and-consumer-trust-summary/;https://www.privacyengine.io/data-privacy-statistics-worldwide/

GenAI exacerbates these vulnerabilities by catalyzing the amplification of threats. Without GenAI, CSOs already face legal repression and funding restrictions. With GenAI, these threats become more systematic and difficult to track. Deepfakes are used as fake “evidence” in the criminalization of activists, chatbots spread scandalous slander that makes donors withdraw support, and bot swarms attack digital accounts of CSOs 24/7.

But the story does not finish at this dead end. The aforementioned research also identifies certain adaptation techniques that demonstrate the continued durability of civil society. Digital cooperative projects like Kolektif.id, which generates independent finances through the sale of items, have surfaced in Indonesia. SIREN (Resilience Information System), a shared data center to track AI buzzers, was established by a collaboration of 32 democratic CSOs. “Lapak Verifikasi,” a citizen-based hoax school that teaches synthetic content detection techniques, was founded by local communities in East Java.

These findings show that stakeholder fragmentation is not an insurmountable obstacle, but rather a challenge that can be answered with innovation and collaboration. When civil society is empowered, not limited, democratic resilience is not only possible, but can become a reality. GenAI may have changed the threat landscape, but with the right strategy, it can also be a catalyst for building a more resilient and equitable information ecosystem.

Resilience Strategy

Amid the systemic threat posed by GenAI, the pressing question that countries in the Asia-Pacific must answer is not just how to protect democracy from information disruption, but how to build sustainable resilience. Democratic resilience does not come from banning technology, but from the ability of civil society, governments, and digital platforms to adapt, collaborate, and create resilient information architectures. In this section, I outline lessons from countries in the region that have demonstrated good practices in addressing the GenAI threat, and formulate strategies that are relevant to the Indonesian context.

Civil Society as the Front Guard

The joint research by Puskapol UI and the Penabulu Foundation above also shows that the main vulnerabilities of Indonesian civil society lie in three areas: repressive regulations, funding crises, and internal fragmentation. The ITE Law and the Mass Organizations Law, which were originally designed to maintain order, are now often used to silence criticism and criminalize digital activism. At the same time, funding from international donors has decreased drastically, while local crowdfunding mechanisms are still vulnerable to digital attacks and blocking. Fragmentation among civil society organizations (CSOs)—both sectorally and geographically—weakens the collective capacity to respond to AI-based disinformation.

However, behind this vulnerability, various adaptive strategies have emerged that show that civil society is not passive. In Indonesia, several CSOs have begun to build digital cooperatives such as Kolektif.id, which raises independent funds through merchandise sales and educational services. A coalition of 32 democratic CSOs formed SIREN (Resilience Information System), a shared data center to track AI buzzer activity and map attack patterns. In East Java, a local community established "Lapak Verifikasi," a citizen-based hoax school that trains synthetic content detection skills. These strategies show that civil society can be at the forefront of building democratic resilience, provided it is given adequate space and support.

Integration of Technology, Regulation, and Community

Important lessons also come from other countries in the Asia-Pacific that have developed innovative approaches to addressing the GenAI threat. In Taiwan, the government is working with startups like Gogolook and Taiwan AI Labs to quickly detect and respond to manipulative content.[20] Taiwan's success lies not only in its technology, but also in the legal legitimacy it gives NGOs to report manipulative content without risking criminalization. Technical communities like hackers and academics are involved in the validation process, creating a participatory and transparent ecosystem.[21]

In Japan, the approach is more focused on evidence-based digital literacy. The country faces a major challenge from AI-based disinformation and is pushing for the development of digital watermarks and digital literacy curricula to identify fake content. The government is working with media outlets like NHK to develop detection systems and public education.[22] Meanwhile, the Philippines is demonstrating the power of civil society coalitions through the #FactsFirstPH alliance, a multi-sectoral initiative involving more than 120 organizations, including Rappler and Interaksyon, to counter disinformation.[23] They have established a rapid verification unit and a vulnerability map to map areas prone to hoaxes based on social data.

[20] https://en.tfc-taiwan.org.tw/en_tfc_286/
[21] Chen-Ling Hung, et. Al. AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election. *Thomson Foundation.* https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf.
[22] https://japannews.yomiuri.co.jp/editorial/yomiuri-editorial/20240309-173523/
[23] https://www.rappler.com/movements/factsfirstph/; https://factsfirst.ph

They created a Rapid Response Unit that can verify viral content in less than an hour, and a Vulnerability Map that maps areas prone to disinformation based on sociological data. Hybrid funding—combining international donors and local crowdfunding—helps reduce dependency and increase sustainability.

Answering Indonesia's Challenges

Based on the data above, and by looking at a number of good practices so far, Indonesia's democratic resilience strategy can be formulated in three main pillars. First, regulations that empower, not limit. Revision of the ITE Law needs to be done to exclude AI content as a legal object that requires a higher standard of proof, to prevent the criminalization of activists. In addition, there needs to be a legal umbrella for efforts to legitimize CSOs as digital literacy trainers, especially in grassroots communities.

Developing financial independence comes in second. Through cooperation between governmental organizations (such as Indonesian Kominfo) and CSOs, a crowdfunding platform tailored to democratic issues might be created, for instance, by connecting databases. However, as a type of social entrepreneurship, NGOs that specialize in misinformation research, like MAFINDO, can offer verification services to commercial media, generating a steady alternative financing stream.

Third, strategic regional collaboration. Indonesia can utilize networks such as those owned by SAIL-CfDS to build the GenAI Threat Database that maps cross-country attack patterns, as well as hold cross-border training between AI detection experts from Taiwan and disinformation analysts from Indonesia. Such collaborations not only strengthen technical capacity, but also build regional solidarity in the face of common threats.

Democratic Resilience is Civil Society Resilience

As Gamboa emphasizes in *Resisting Backsliding,* democracies survive when opposition and civil society are able to build collective shields against information disruption. In the GenAI era, these shields cannot simply be regulations or technologies, but must be rooted in the capacity of communities to produce, verify, and disseminate credible information. Democratic resilience is not the result of top-down policies alone, but of an information architecture centered on civil society—where truth is the norm, collaboration is the strategy, and digital sovereignty is the shared goal.

Building an Asia-Pacific Democracy Information Architecture

Amid the transnational threats posed by GenAI, the need for a resilient and collaborative information architecture has never been more urgent. Democracy cannot survive on reactive regulation or fragmented sectoral approaches. It needs a new foundation—an information architecture that not only protects but also empowers civil society, is adaptive to technological innovation, and is regionally connected. This section proposes a framework for an evidence-based and cross-actor collaborative democracy information architecture, drawing on best practices in the Asia-Pacific and findings from field research in Indonesia.

Basic Principles: Evidence-Based Collective Architecture

A democratic information architecture must be built on three core principles. *First*, it must empower civil society, not constrain it. My research discussed above shows that civil society organizations (CSOs) face regulatory pressures, funding crises, and internal fragmentation. An effective architecture must respond to these vulnerabilities by creating safe spaces and structural support for CSOs to operate independently and collaboratively.

Second, it must adapt to the speed of GenAI innovation. Static regulation is not enough to deal with evolving technology. Flexible mechanisms, based on real-time data, and able to respond to threats quickly and measurably are needed.

Third, a democratic information architecture must be regionally networked. The GenAI threat is transboundary, so an effective response must involve cross-country cooperation, knowledge exchange, and policy harmonization.

And *fourth,* this information architecture must be multi-stakeholder, meaning it involves various actors (governments, CSOs, technology platforms, academics, mass media, and others) in a collaborative environment.

Responsive Regulation and Healthy Ecosystems

At the national level, regulatory reform is a crucial first step. One concrete proposal that I can convey is a moratorium on the use of the ITE Law and the Mass Organizations Law against political GenAI content, until an independent tribunal consisting of academics, human rights practitioners, and AI experts is formed. This model is inspired by the Philippines, where the Supreme Court initiated major reforms in the digital justice system through the Strategic Plan for Judicial Innovations 2022–2027. In a speech at the Manila Tech Summit 2024, Senior

Associate Justice Marvic Leonen emphasized the importance of the legal system to keep up with developments in AI, including in dealing with the challenges of disinformation and digital rights violations. He called for cooperation between the courts and the technology community to formulate more definitive rules regarding the use of AI in legal processes. This statement shows that the Philippines is moving towards establishing a legal framework that is more adaptive to digital technology, including the possibility of establishing a special body or mechanism to handle digital rights and AI issues.

In addition, there needs to be legal protection for whistleblowers and activists who report AI-based disinformation. Without legal guarantees, reporting will be hampered by fear and the risk of criminalization, even though they are key actors in maintaining the integrity of information.

In terms of funding, an endowment fund from the government and private donors, with tax incentives for companies that contribute, is needed. A verified crowdfunding platform can also be developed through collaboration between Kominfo and CSOs, for example by integrating Kitabisa.com with the SAIL database for digital literacy projects and local advocacy.

To strengthen cross-actor coordination, Indonesia can form a collaborative command center involving the government (such as BSSN and KPU), CSOs (such as Mafindo and LBH Pers), and technology platforms (such as Meta and Google). SAIRAP can carry out three main functions: verification of AI content in less than an hour, integrated reporting of GenAI threats, and AI literacy training for vulnerable communities such as farmers, laborers, and women—the groups identified as most vulnerable in my research above.

Asia-Pacific Resilience Network

At the regional level, universities and research institutions can act as regional intelligence hubs, developing a real-time database that maps GenAI attack patterns, digital fingerprints, and actors involved. This dashboard can be complemented by an early warning system and a repository of best practices from member countries, such as Japan's literacy module or Taiwan's funding model.

In addition, a cross-border expert team consisting of (for example) an AI detector from Taiwan, a disinformation analyst from Indonesia, and a regulator from South Korea is needed. This team can simulate GenAI attacks and test the resilience of information systems in different countries, while strengthening technical and diplomatic capacity.

Universities and research institutions are in a strategic position to be catalysts in building a democratic information architecture. They can create an index that measures the threat detection capacity, CSO strength, and regulatory framework in each country. In addition, they can facilitate a regular forum connecting CSOs, governments, and technology platforms (such as Google).

As knowledge hubs, universities can also organize certification training for activists, public officials, and technologists who are trained in threat detection, policy advocacy, and funding management. With this integrative approach, the democratic information architecture becomes not just a defensive wall, but a living network that connects democratic actors in solidarity and innovation.

Conclusion

The Asia-Pacific region's democracy faces structural, epistemological, and technical challenges. GenAI's extensive, hyper-realistic, and international information manipulation has sped up the erosion of democracy. It reduces civic space, erodes social cohesiveness, and ruins the legitimacy of institutions. In this perspective, the major aim of GenAI's disruption of democracy is no longer elections, but rather the everyday democratic life, from policy discourse to public involvement.

This paper's main argument is that technology and legislation alone cannot create democratic resilience. It necessitates an evidence-based, regionally integrated, civil society-centered information architecture. This study makes the case that information manipulation is a fundamental mechanism of democratic decline and that creating credible alternative information is necessary to counter it, drawing on the work of Applebaum, Levitsky & Way, and Gamboa.

In the future, civic society must be the primary defender of information integrity. This entails developing cross-issue alliances, enhancing verification capabilities, and creating innovative independent funding. Regulations must be changed by governments to prevent them from being used as instruments of repression, and online companies must answer for the algorithms they use. Addressing the transnational danger of GenAI at the regional level requires cross-border cooperation and knowledge sharing.

A dynamic democracy can change with the times. Rebuilding public trust through a robust, equitable, and inclusive information ecosystem must be the first step in adapting to the GenAI future.

References

Applebaum, A. (2020). Twilight of Democracy: The Seductive Lure of Authoritarianism. New York: Doubleday.

Applebaum, A. (2024). Autocracy, Inc.: The Dictators Who Want to Run the World. London: Penguin Books Limited.

Brookings Institution. (2024). Indonesia's election reveals its democratic challenges. Retrieved from https://www.brookings.edu/articles/indonesias-election-reveals-its-democratic-challenges/

Brookings Institution. (2024). Why Indonesia's Democracy Is in Danger. Journal of Democracy. Retrieved from https://www.journalofdemocracy.org/onlineexclusive/why-indonesias-democracy-is-in-danger/

Channel News Asia. (2024). AI disinformation & deepfakes in Indonesia elections. Retrieved from https://www.channelnewsasia.com/asia/ai-disinformation-deepfakes-indonesia-elections-4091296

Chen-Ling Hung, et al. (2024). AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election. Thomson Foundation. Retrieved from https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf

CNN. (2024). India's election campaign turns negative as Modi and ruling party embrace Islamophobic rhetoric. Retrieved from https://edition.cnn.com/2024/05/28/india/india-narendra-modi-hate-speech-analysis-intl-hnk/index.html

CNN. (2024). Suharto deepfake AI scam in Indonesia election. Retrieved from https://edition.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl/index.html

Csernatoni, R. (2024). Can Democracy Survive the Disruptive Power of AI? Carnegie Endowement for International Peace https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

Gamboa, L. (2022). Resisting Backsliding: Opposition Strategies against the Erosion of Democracy. Cambridge: Cambridge University Press.

Habermas, J. (1989). The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. Cambridge, MA: MIT Press. (Original work published 1962)

Hung, C.-L., et al. (2024). AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election. Thomson Foundation.

Jaswal, S. (2024). Inside the BJP’s WhatsApp Machine. Pulitzer Center. Retrieved from https://pulitzercenter.org/stories/inside-bjpswhatsapp-machine

Levitsky, S., & Way, L. A. (2023). Democracy’s Surprising Resilience. Journal of Democracy, 34(4), 5–20.

Microsoft Threat Intelligence. (2023). Microsoft Digital Defense Report: Building and improving cyber resilience. Retrieved from https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Mogul, R. (2024). India’s election campaign turns negative. CNN. Retrieved from https://edition.cnn.com/2024/05/28/india/india-narendra-modi-hate-speech-analysis-intl-hnk/index.html

PrivacyEngine. (2024). Data Privacy Statistics Worldwide. Retrieved from https://www.privacyengine.io/dataprivacy-statistics-worldwide/

Puskapol UI. (2024). Analisis Sosial terhadap Kondisi Ekosistem Ruang Sipil dan Kerentanan Masyarakat Sipil di Indonesia. Interim report. Puskapol UI & Yayasan Penabulu.

Rappler. (2024). FactsFirstPH. Retrieved from https://www.rappler.com/movements/factsfirstph/

Rosadi, S. D. (2024). The Use of AI and Social Media for ‘Black Campaign’ in the 2024 General Elections in Indonesia: A Review of Indonesian Laws on Black Campaign. Majority World Initiative Papers. Yale Law School. Retrieved from https://law.yale.edu/sites/default/files/area/center/isp/documents/mwi-sinta-dewi-rosadi_2024-08-01_re-fin.pdf

Sharma, Y. (2024). ‘Infiltrators’: Modi accused of anti-Muslim hate speech amid India election. Al Jazeera. Retrieved from https://www.aljazeera.com/news/2024/4/22/infiltrators-modi-accused-of-anti-muslim-hate-speech-amid-indiaelection

Singapore HTX. (2024). Sensemaking & Surveillance. Retrieved from https://www.htx.gov.sg/who-we-are/what-we-do/our-expertise/sense-making-surveillance

Staqu Technologies. (2024). Trinetra 2.0 AI-powered surveillance system. Retrieved from https://cxotoday.com/press-release/staqu-collaborates-with-up-police-to-launch-ai-powered-trinetra-2-0featuring-new-crime-gpt-feature/

Supreme Court of the Philippines. (2024). SAJ Leonen: Legal system should keep abreast with AI developments. Retrieved from https://sc.judiciary.gov.ph/saj-leonen-despite-risks-legal-system-should-keep-abreast-with-ai-developments/

Thomson Foundation. (2024). AI and Disinformation in Taiwan's 2024 Election. Retrieved from https://www.thomsonfoundation.org/latest/ai-and-disinformation-in-taiwan-s-2024-election/

Yomiuri Shimbun. (2024). Editorial on digital watermarking and literacy. Retrieved from https://japannews.yomiuri.co.jp/editorial/yomiuri-editorial/20240309-173523/

Authenticity and The Use of AI

This article is based on my concepts, which were refined through the examination of several critical sources as detailed in the content. This work is completely original with no instances of plagiarism. Every source that was used has been properly cited. Unless otherwise noted, web research was used to gather the data used in this paper. To validate data and strengthen notions, I used a number of AI tools, such as Consensus, Copilot, and DeepSeek. To improve the paper's presentation, I also used QuillBot and Grammarly.

INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience in the Asia-Pacific: Actions and Adaptations

↘ Faculty of Social and Political Sciences
Universitas Gadjah Mada

↘ 21 August 2025

saferinternetlab.org/iris @saferinetlab @cfds_ugm iris@saferinternetlab.org