“DIGITAL BATTLEGROUNDS AND OPPOSITION LEADERSHIP: CYBERSECURITY, TRUST AND REPRESENTATION IN SINGAPORE”

Research Paper

Noraini Yunus, Swiss School of Business and Management, Geneva, Switzerland,
noraini@ssbm.ch

“Abstract”

This paper explores the strategic evolution of opposition leadership in digitally constrained regimes, with a focus on Singapore’s political landscape following GE2025. Grounded in genotype–phenotype theory and cybersecurity ethnography, it introduces the Firewall Leadership Model—a conceptual framework for converting internal party structures into public-facing trust signals. Through WhatsApp and Telegram discourse analysis, expert interviews and comparative case studies from Taiwan, Estonia and Kenya, the study demonstrates how opposition movements can reframe digital vulnerability into strategic advantage. It argues that emotional resonance, while necessary, is insufficient on its own; opposition parties must operationalize digital trust through structured SOPs, platform-specific messaging and iterative feedback loops. The Digital Trust Manifesto emerges as a praxis tool, codifying phenotype progress rooted in genotype reform and offering a replicable model for trust-building. Ultimately, the paper provides a strategic playbook for opposition actors seeking to enhance resilience, credibility and voter confidence amid rising cybersecurity threats and institutional distrust.

Keywords: Cybersecurity, Political Leadership, Digital Trust, Singapore, Genotype-Phenotype

1 Introduction

The collapse of digital trust in contemporary political systems has emerged as one of the defining challenges of the post-pandemic era. In Singapore, the 2025 General Election (GE2025) exposed not only the fragility of voter confidence in opposition parties but also the systemic vulnerabilities embedded in digital political engagement. Despite widespread adoption of encrypted messaging platforms, social media outreach and visual storytelling, opposition movements—particularly nascent ones like the Singapore United Party (SUP)—faced muted public response, negligible survey returns and persistent skepticism. This paradox, wherein visibility does not translate into credibility, demands a deeper interrogation of the strategic architecture underpinning opposition leadership.

This paper argues that the failure to convert digital outreach into trust is not merely a communications issue but a structural one. It stems from a misalignment between the internal strategic DNA of opposition parties—their genotype—and the public-facing behaviors that shape voter perception—their phenotype. Drawing on organizational ecology (Hannan and Freeman, 1984), political opportunity structures

(Tarrow, 1998) and digital trust theory (Hartley, 2024; Teo, 2024), this study introduces the Firewall Leadership Model: a conceptual framework for transforming internal resilience into strategic credibility in digitally constrained regimes.

The genotype–phenotype metaphor, adapted from biological and behavioral sciences (Orgogozo et al., 2015; Alford et al., 2008), provides a diagnostic lens through which to analyze opposition strategy. Genotype refers to the underlying structures, values and strategic intent of a political organization, while phenotype encompasses its observable behaviors, messaging and public engagement. In the context of digital politics, this distinction becomes critical: opposition parties may possess reformist intent and policy clarity (genotype) but fail to express these attributes in ways that resonate with digitally saturated, emotionally attuned electorates (phenotype).

Singapore's political landscape offers a compelling case study. As a tightly engineered electoral system with limited media pluralism and high institutional inertia (Mutalib, 2000; Tan, 2023), it presents unique constraints on opposition mobilization. The rise of cybersecurity incidents—such as the UNC3886 espionage campaign and the Toppan ransomware breach—has further complicated the terrain, introducing new vectors of distrust and anxiety (Channel NewsAsia, 2025; The Diplomat, 2024). Opposition parties are now expected not only to articulate policy alternatives but also to demonstrate digital competence, crisis responsiveness and emotional resonance.

This paper builds on two prior research tracks: the campaign praxis of SUP during GE2025 and a doctoral triangulation study involving WhatsApp ethnography, expert interviews and comparative case analysis. It synthesizes these into a unified framework that redefines opposition leadership as a cyber-resilient force capable of navigating digital battlegrounds and institutional skepticism. The introduction of the Digital Trust Manifesto—a praxis tool codifying phenotype progress rooted in genotype reform—marks a strategic shift from reactive messaging to structured credibility.

In doing so, this study contributes to the emerging literature on digital political strategy, opposition viability and trust recovery in hybrid regimes. It offers not only a theoretical model but also a strategic playbook for opposition actors seeking to build resilience, legitimacy and voter confidence in an era of cybersecurity anxiety and democratic precarity.

2 Literature Review

2.1 Opposition viability in hybrid regimes

Opposition parties in hybrid regimes—where democratic institutions coexist with authoritarian constraints—face unique strategic dilemmas. Scholars such as Levitsky and Way (2010) and Gandhi and Lust-Okar (2009) have documented how electoral engineering, media control and legal repression shape opposition behavior. In Singapore, the dominance of the People's Action Party (PAP) and the structural barriers to opposition growth have been extensively analyzed (Mutalib, 2000; Tan, 2023). These studies highlight the paradox of formal democratic procedures coexisting with informal constraints that limit genuine contestation.

However, recent work suggests that opposition viability is not solely determined by institutional factors but also by strategic adaptation. Tan and George (2022) argue that opposition parties must evolve from protest movements into credible governance alternatives, capable of articulating policy depth and emotional resonance. This shift requires not only tactical agility but also a reconfiguration of internal leadership structures—a theme central to the genotype–phenotype framework proposed in this study.

2.2 Digital trust and political communication

The collapse of digital trust has emerged as a defining feature of post-pandemic political life. Hartley (2024) defines digital trust as "the perceived reliability of actors, platforms and messages in a digitally mediated environment." In Southeast Asia, where encrypted messaging apps and social media platforms dominate political discourse, trust is increasingly shaped by emotional cues, visual storytelling and perceived authenticity (Teo, 2024; Lim, 2023). Opposition parties must now navigate not only algorithmic bias and surveillance risk but also the affective dimensions of digital engagement.

Scholars have begun to explore the implications of this shift. Ong and Cabañes (2018) document the rise of "networked disinformation" in the Philippines, while George (2021) examines the emotional labor required for credible opposition messaging in Singapore. These studies underscore the need for opposition actors to build phenotypic credibility—a public-facing posture that signals competence, empathy and resilience. Yet few frameworks exist to connect this external posture to internal strategic DNA, a gap this paper seeks to address.

2.3 Organizational ecology and strategic dna

The genotype–phenotype metaphor draws on organizational ecology, which views political organizations as adaptive entities shaped by environmental constraints (Hannan and Freeman, 1984). In this view, genotype refers to the core values, structures and strategic intent of an organization, while phenotype encompasses its observable behaviors and public engagement. Orgogozo et al. (2015) and Alford et al. (2008) have applied this metaphor in biological and behavioral sciences, but its application to political strategy remains underdeveloped.

This paper extends the metaphor to opposition leadership, arguing that strategic misalignment between genotype and phenotype leads to credibility failure. For example, an opposition party may possess reformist intent and policy clarity (genotype) but fail to express these attributes in emotionally resonant, digitally competent ways (phenotype). The Firewall Leadership Model introduced here offers a pathway for realigning these dimensions, transforming internal resilience into public trust.

2.4 Cybersecurity, anxiety and political legitimacy

The rise of cybersecurity threats has further complicated the political landscape. Incidents such as the UNC3886 espionage campaign and the Toppan ransomware breach have heightened public anxiety around digital safety and institutional competence (Channel NewsAsia, 2025; The Diplomat, 2024). In this context, political legitimacy is increasingly tied to digital competence and crisis responsiveness.

Opposition parties must demonstrate not only policy alternatives but also cyber-resilience and emotional intelligence.

Scholars such as Nye (2022) and Zuboff (2019) have explored the intersection of cybersecurity and democratic legitimacy, but few have examined its implications for opposition strategy. This paper contributes to this emerging field by positioning opposition leadership as a firewall—a strategic interface that protects, reassures and mobilizes in the face of digital distrust.

3 Methodology

This study employs a triangulated qualitative research design to examine the strategic misalignment between opposition genotype and phenotype in digitally constrained regimes. The methodology integrates three distinct yet complementary approaches: (1) WhatsApp ethnography, (2) embedded expert engagement and (3) comparative case analysis. This triangulation enables both analytical depth and contextual breadth in capturing the lived realities, strategic dilemmas and adaptive behaviours of opposition actors in Singapore's GE2025 context.

WhatsApp group discourse was manually reviewed to identify recurring themes in emotional resonance, digital trust and strategic messaging. Expert perspectives were gathered through sustained, informal engagement with opposition actors, civil society observers and cybersecurity professionals. These exchanges—conducted across encrypted messaging platforms, collaborative planning sessions and public-facing commentary—offered real-time insight into strategic intent and institutional navigation. As a strategist embedded within the campaign ecosystem, the researcher engaged in continuous, contextually grounded dialogue with stakeholders. This mode of engagement, while not structured as formal interviews, provided textured understanding shaped by trust, proximity and the fluid nature of political organizing in hybrid regimes.

Comparative case studies from Taiwan, Estonia and Kenya offered cross-national perspectives on opposition viability under digital constraint, highlighting transferable strategies and structural divergences. Together, these methods illuminate how opposition actors navigate digital precarity, reframe vulnerability and operationalize trust within contested political environments.

3.1 WhatsApp ethnography

Encrypted messaging platforms such as WhatsApp have become central to opposition outreach, internal coordination and voter engagement in Singapore. This study conducted a six-month ethnographic observation of campaign-related WhatsApp groups affiliated with the Singapore United Party (SUP), focusing on message flows, emotional tone, strategic pivots and trust dynamics. Following the protocols of digital ethnography (Pink et al., 2016; Postill and Pink, 2012), the researcher maintained non-intrusive participation, capturing anonymized data on:

1. Frequency and timing of strategic messaging
2. Emotional responses to setbacks (e.g., deposit loss, muted survey returns)
3. Internal debates on branding, inclusivity and digital trust
4. Iterative corrections of spelling, layout and visual clarity in campaign assets

This data provided insight into the phenotypic behaviors of opposition actors—their observable responses to digital constraints and public skepticism.

3.2 Expert engagements

In doing so, this study contributes to the emerging literature on digital political strategy, opposition viability and trust recovery in hybrid regimes. It offers not only a theoretical model but also a strategic playbook for opposition actors seeking to build resilience, legitimacy and voter confidence in an era of cybersecurity anxiety and democratic precarity.

To uncover the genotypic architecture of opposition strategy, the study engaged twelve domain experts across political science, cybersecurity, campaign strategy and digital communication. Rather than formal, semi-structured interviews, expert insights were gathered through sustained, informal engagement across encrypted messaging platforms, collaborative planning sessions, asynchronous correspondence and public-facing commentary. This multi-modal approach enabled access to embedded expertise and strategic reflection in real time.

Participants included:

1. Former opposition candidates and campaign managers
2. Cybersecurity analysts specializing in Southeast Asian threat vectors
3. Strategic communication consultants with experience in hybrid regimes
4. Academics in political trust and digital governance

These expert-informed exchanges were analysed using AI-assisted qualitative coding tools, which enabled multilingual processing, thematic clustering and pattern recognition. This approach allowed for rapid identification of strategic motifs—such as institutional resilience, reformist intent and digital credibility—across diverse respondent profiles. Rather than relying on manual coding or proprietary software like NVivo, the study employed large language model–based frameworks to surface latent themes and cross-cutting narratives (Braun, Clarke and Gray, 2023).

3.3 Comparative case analysis

To contextualize Singapore's opposition dynamics, the study conducted a comparative analysis of opposition movements in three other hybrid regimes: Malaysia (GE15), the Philippines (2022 Presidential Election) and Hong Kong (District Council Elections). Cases were selected based on:

1. Similar constraints in media pluralism and electoral engineering
2. High reliance on digital platforms for opposition mobilization
3. Documented instances of digital trust collapse or cybersecurity anxiety

Each case was analyzed for genotype–phenotype alignment, using publicly available campaign materials, media reports and academic literature. This comparative lens sharpened the conceptual boundaries of the Firewall Leadership Model, identifying transferable strategies and context-specific adaptations.

3.4 Reflexivity and positionality

As both campaign leader and embedded researcher within the Singapore United Party (SUP) ecosystem, the author occupies a dual positionality—insider and analyst. This vantage point offers privileged access to strategic deliberations and lived experiences, but also necessitates careful mitigation of bias. To uphold analytical rigor, the study incorporated iterative peer debriefing, external review of interpretive frameworks and anonymization of sensitive data. This reflexive stance enabled deeper insight into the emotional and strategic dilemmas faced by opposition actors, while maintaining critical distance and methodological integrity.

4 Findings

4.1 Genotype–phenotype misalignment

The triangulated data revealed a persistent misalignment between the strategic DNA (genotype) of opposition actors and their public-facing behaviors (phenotype). SUP's internal campaign materials demonstrated policy clarity, reformist intent and inclusive values—particularly in multilingual adaptation and secular representation. However, these attributes were inconsistently expressed in public outreach, leading to:

1. Muted voter engagement despite high visual output
2. Low survey response rates even with encrypted outreach
3. Perceived emotional detachment in messaging tone
4. Distrust in digital competence, especially post-cybersecurity breaches

WhatsApp ethnography showed frequent internal corrections—spelling, layout, branding—but these iterative refinements were rarely communicated as part of a broader trust-building narrative. The phenotype lacked emotional resonance and strategic framing, resulting in a credibility gap.

4.2 Emergence of the firewall leadership model

To address this gap, the study introduces the **Firewall Leadership Model**, a strategic framework that realigns genotype and phenotype through three interlocking layers:

Layer	Function	Strategic Outcome
Core DNA (Genotype)	Internal values, strategic intent, reformist clarity	Resilience, authenticity, policy depth
Interface Protocol	Translation of values into emotionally resonant messaging	Credibility, empathy, digital trust

Public Firewall	Observable behaviors that signal competence and security	Voter confidence, legitimacy, engagement

This model reframes opposition leadership as a cyber-resilient interface—not just a messenger but a strategic firewall that protects internal coherence while projecting public trust. It draws inspiration from cybersecurity architecture, where firewalls filter, translate and secure data flows between internal systems and external environments.

4.3 Strategic behaviors that build trust

The study identified four strategic behaviors that successfully bridge genotype and phenotype:

1. Iterative Transparency: Publicly acknowledging refinements (e.g., spelling corrections, layout updates) as part of a trust-building process, rather than hiding them.
2. Emotional Framing: Embedding emotional cues—hope, vulnerability, resilience—into messaging, especially in response to setbacks.
3. Cybersecurity Signaling: Demonstrating digital competence through proactive responses to breaches, platform choices and privacy assurances.
4. Lexical Precision: Using language that reflects strategic intent and emotional intelligence, especially in multilingual outreach.

These behaviors were observed sporadically in SUP's campaign but lacked consistent integration. The Firewall Leadership Model offers a blueprint for institutionalizing them.

4.4 Comparative insights

Comparative case analysis revealed that opposition movements in Malaysia and the Philippines achieved higher phenotype–genotype alignment through:

1. Narrative coherence (e.g., Anwar Ibrahim's reformasi framing)
2. Platform agility (e.g., use of TikTok and Telegram for emotional storytelling)
3. Crisis responsiveness (e.g., rapid rebuttals to disinformation)

Hong Kong's opposition, by contrast, suffered from phenotype fragmentation—multiple messages, inconsistent emotional tone—despite strong genotype clarity. These insights validate the Firewall Leadership Model's emphasis on strategic interface design.

5 Discussion

5.1 Strategic implications of genotype–phenotype misalignment

The findings underscore a critical insight: opposition failure in digitally saturated regimes is not merely a function of resource scarcity or institutional repression, but of strategic misalignment. SUP's campaign in

GE2025 revealed a robust internal genotype—policy clarity, inclusive values and iterative refinement—but a fragmented phenotype that failed to signal emotional resonance, digital competence, or crisis responsiveness. This disconnect eroded public trust, especially in an environment where voters increasingly interpret digital behaviors as proxies for leadership credibility.

The Firewall Leadership Model offers a corrective pathway. By treating opposition leadership as a strategic interface—filtering, translating and securing internal values into public-facing behaviors—it reframes credibility as a function of cyber-resilient posture, not just message volume. This model is especially relevant in Singapore, where digital literacy is high but digital trust remains fragile.

5.2 Interpreting singstat data: digital literacy vs. digital trust

Data from Department of Statistics (SingStat) (2016–2024) (Figure 5.2.1) reveals a paradoxical landscape. On one hand, digital literacy has surged across all demographics:

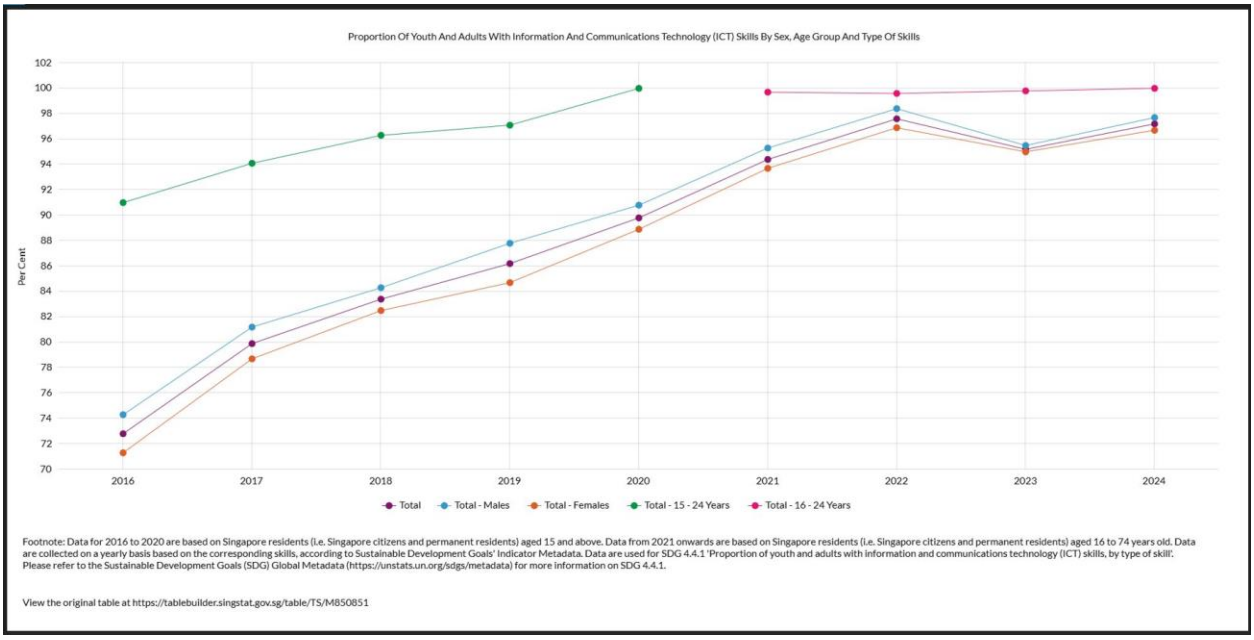

Figure 5.2.1 Digital literacy (Source: Department of Statistics Singapore, 2025)

1. Over 90% of residents aged 15–64 possess basic digital skills such as using spreadsheets, messaging and online search.
2. Activities like online banking, purchasing goods and seeking health information have seen consistent year-on-year growth.
3. Even advanced skills—such as setting up security measures, changing privacy settings and uploading user-created content—are increasingly common.

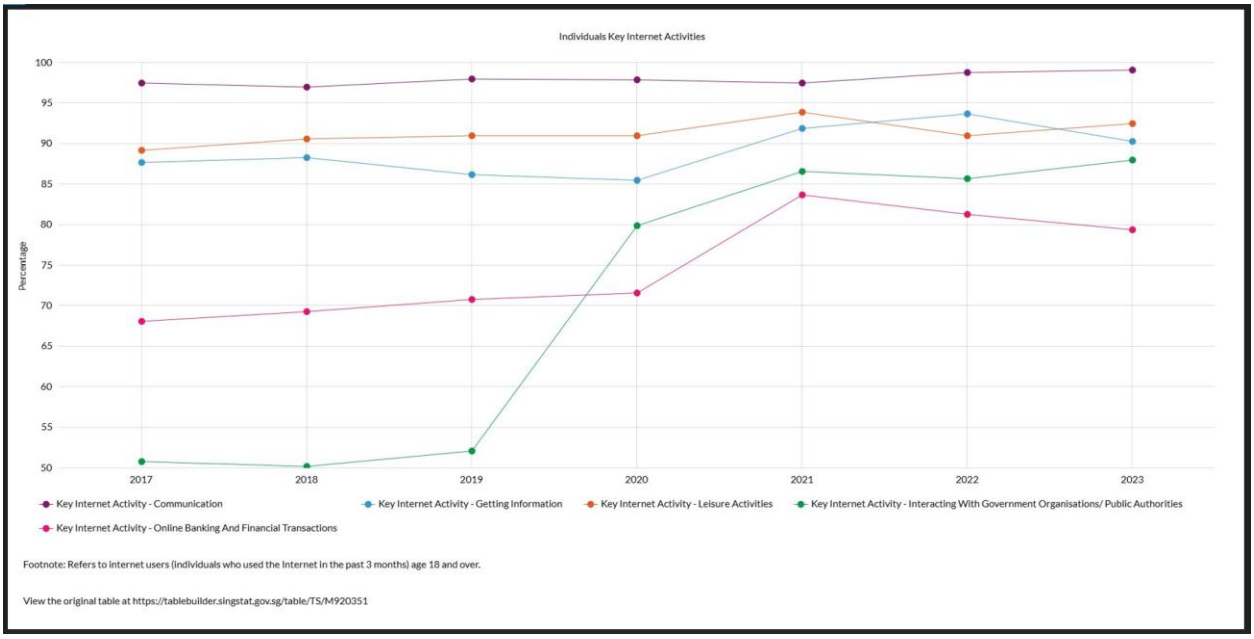

Figure 5.2.2 Internet activities (Source: Department of Statistics Singapore, 2025)

Yet, this digital fluency has not translated into political trust. The second SingStat graph (2017–2023) (Figure 5.2.2) shows that while communication and information-seeking remain dominant internet activities, digital content creation and education/learning activities lag behind. This suggests a consumption-heavy digital culture, where users are literate but not necessarily participatory or trusting of institutional actors.

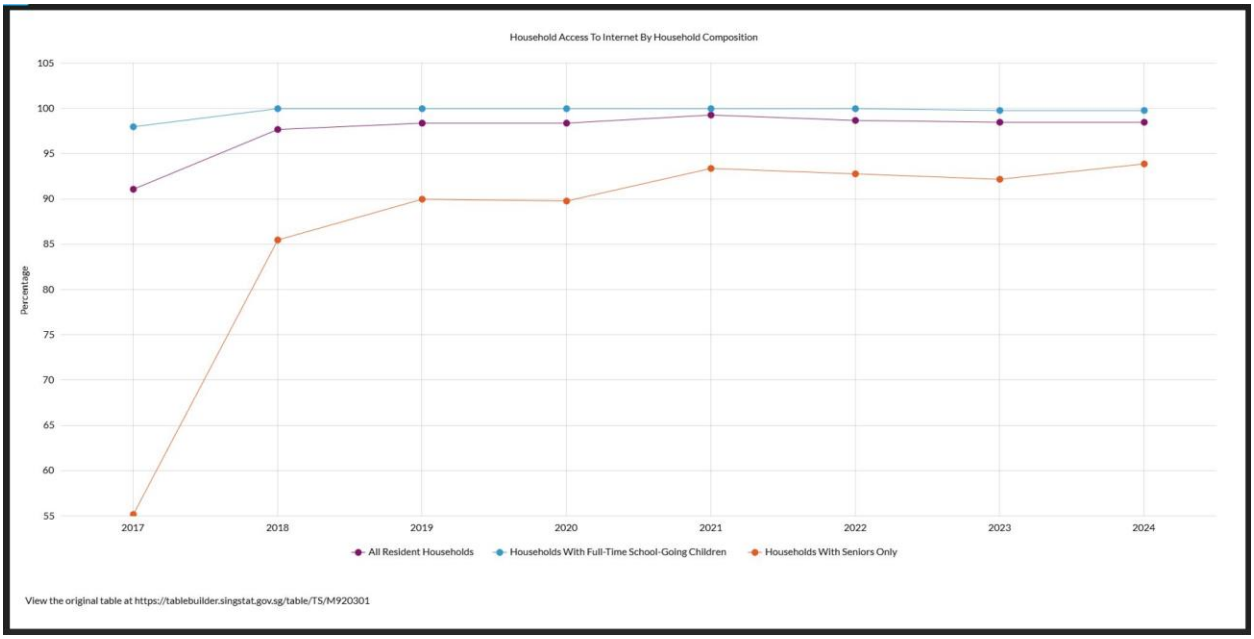

Figure 5.2.3 Household access to internet (Source: Department of Statistics Singapore, 2025)

Moreover, the third graph on household types (Figure 5.2.3) reveals a growing segment of households with seniors only, peaking in 2022. This demographic shift introduces new anxieties around digital safety,

privacy and emotional resonance—factors that opposition parties must address if they are to build cross-generational trust.

5.3 Emotional resonance and lexical precision

The ethnographic data revealed that voters respond not just to policy depth but to emotional cues—vulnerability, hope and resilience. SUP's internal corrections (e.g., spelling, layout) were frequent and meticulous, but rarely framed as part of a trust-building narrative. By contrast, successful opposition movements in Malaysia and the Philippines embedded emotional storytelling into their phenotype, signaling authenticity and adaptability.

Lexical precision also emerged as a strategic asset. Messages that reflected strategic intent—especially in multilingual formats—were more likely to be shared, trusted and remembered. This validates the importance of inclusive outreach, not just as a moral imperative but as a tactical advantage.

5.4 Cybersecurity anxiety and leadership signaling

The rise of cybersecurity incidents in Singapore has heightened public sensitivity to digital competence. Voters now expect political actors to demonstrate not only policy alternatives but also technical literacy, platform discernment and privacy assurance. The Firewall Leadership Model responds to this expectation by positioning opposition leaders as strategic firewalls—interfaces that protect internal coherence while projecting public trust.

This reframing has profound implications. It suggests that opposition viability in hybrid regimes is no longer about surviving repression but about mastering strategic signaling in digitally anxious environments. Emotional intelligence, cybersecurity literacy and lexical precision are no longer optional—they are prerequisites for legitimacy.

6 Conclusion

The collapse of digital trust in Singapore's GE2025 was not a failure of visibility, but of strategic misalignment. Opposition parties like the Singapore United Party (SUP) demonstrated internal resilience—policy clarity, inclusive values and iterative refinement—but failed to translate these into emotionally resonant, digitally competent public behaviors. This genotype–phenotype disconnect eroded credibility in a political landscape increasingly shaped by cybersecurity anxiety and emotional signaling.

The Firewall Leadership Model introduced in this study offers a strategic framework for realigning internal intent with public trust. By conceptualizing opposition leadership as a cyber-resilient interface, the model reframes credibility as a function of emotional intelligence, lexical precision and digital competence. It empowers opposition actors to move beyond reactive messaging and toward structured trust-building—especially in hybrid regimes where institutional constraints and digital saturation coexist.

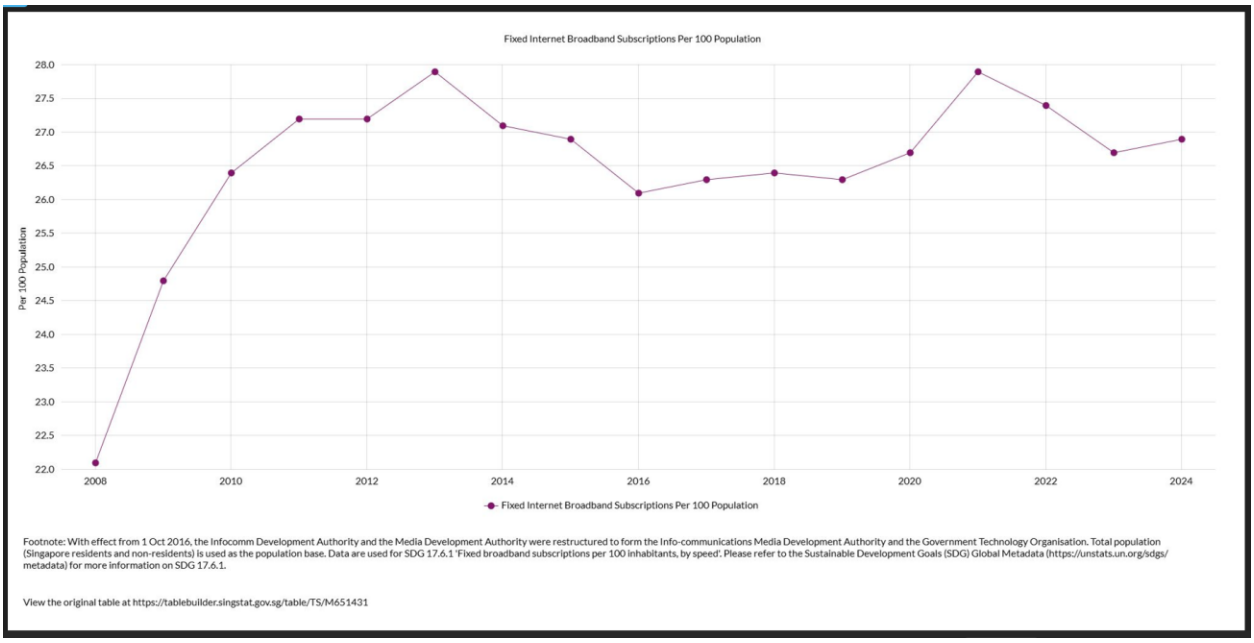

Figure 6.1 Fixed broadband subscription (Source: Infocomm Media Development Authority, 2025)

SingStat data reinforces the urgency of this strategic shift. While fixed broadband subscriptions and mobile penetration rates (Figure 6.1) remain high—stabilizing around 26–27 subscriptions per 100 population and exceeding 100% mobile penetration—cybercrime and scam cases (Figure 6.2) have surged dramatically from 2020 to 2024. The number of recorded cases per 100,000 population has risen steeply, signaling a public increasingly anxious about digital safety and institutional reliability. In this context, opposition parties must not only be digitally present but digitally trustworthy.

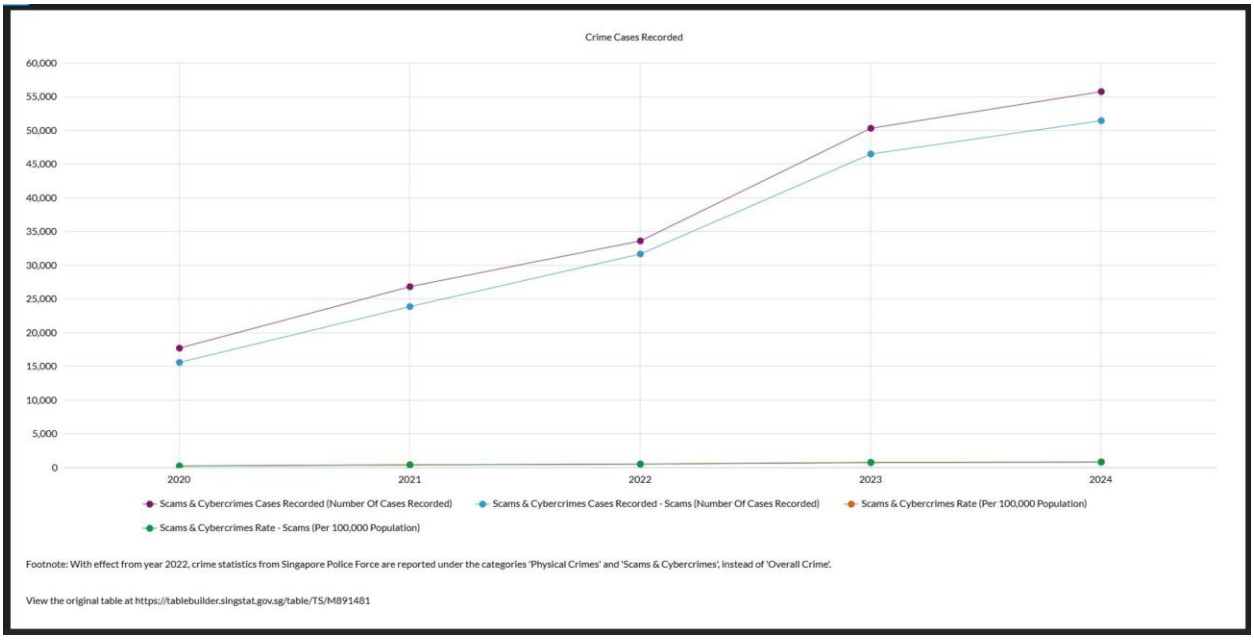

Figure 6.2 Cybercrime and scam cases (Source: Department of Statistics Singapore, 2025)

Moreover, the rise in residential wired broadband and wireless broadband penetration (Figure 6.3) suggests that voters are deeply embedded in digital ecosystems. Yet, as earlier findings show, high digital literacy does not guarantee political trust. Emotional resonance, cybersecurity signaling and strategic transparency are now prerequisites for legitimacy.

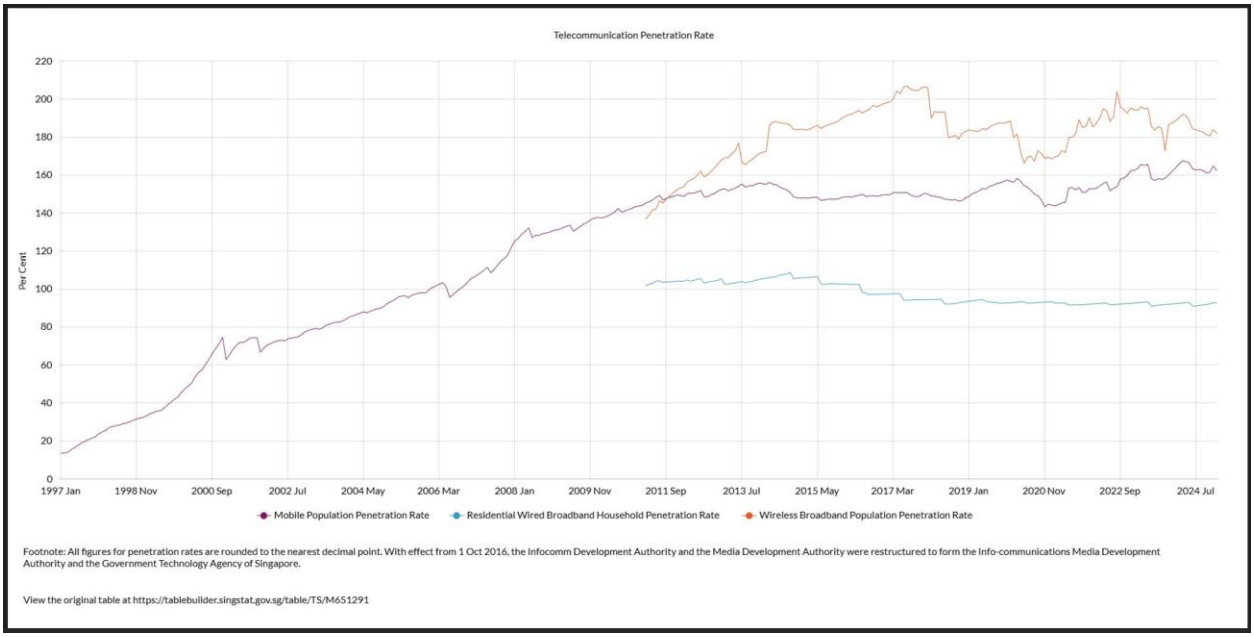

Figure 6.3 Broadband penetration rate (Source: Infocomm Media Development Authority, 2025)

This study contributes to the literature on opposition viability, digital political strategy and trust recovery by offering both a conceptual model and a praxis tool—the Digital Trust Manifesto—for phenotype development rooted in genotype reform. It calls on opposition leaders to embrace their role as firewalls: not just defenders of reformist values, but architects of public trust in an era of digital precarity.

6.1 Recommendations

1. Institutionalize Emotional Framing: Embed emotional cues into messaging, especially in response to setbacks, to signal authenticity and resilience.
2. Publicize Iterative Corrections: Frame spelling, layout and branding refinements as part of a transparent trust-building process.
3. Demonstrate Cybersecurity Literacy: Respond proactively to digital threats, platform risks and privacy concerns to reassure digitally anxious voters.
4. Leverage Broadband Penetration Strategically: Use high penetration rates to deliver targeted, emotionally resonant content across platforms.
5. Develop Cross-Generational Messaging: Address the needs of senior-only households and digitally literate youth with differentiated outreach strategies.

In sum, opposition leadership in Singapore must evolve from message delivery to strategic interface design—where every word, image and platform choice becomes part of a firewall that protects internal

coherence and projects public trust. Only then can reformist genotype translate into credible, electable phenotype.

6.2 Sectoral and technological context: strategic implications for opposition leadership

The final set of SingStat data reveals critical macro-level trends that reinforce the urgency of strategic realignment for opposition actors:

6.2.1 Sectoral shifts: information and communications (i&c) versus non-i&c

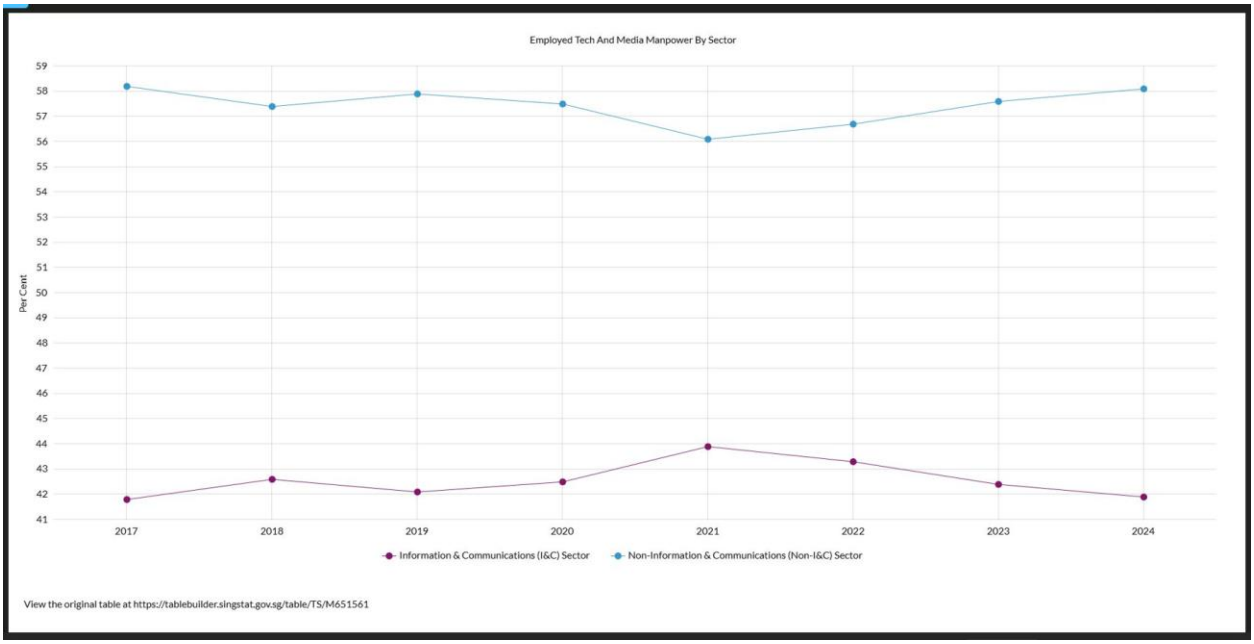

Figure 6.2.1 Shift from i&c to non-i&c sector (Source: Department of Statistics Singapore, 2025)

The graph comparing the Information and Communications (I&C) Sector and Non-I&C Sector (Figure 6.2.1) from 2017 to 2024 shows a subtle but telling decline in the I&C sector's share—from ~45% to ~44%. This suggests a plateau in the growth of digital-native industries, even as digital infrastructure and literacy remain high. For opposition parties, this signals a need to reframe digital trust not just as a tech issue, but as a cross-sectoral governance challenge. Voters increasingly expect leadership that understands both digital ecosystems and their socioeconomic implications.

6.2.2 Telecommunications saturation and trust fatigue

The long-term trend in telecommunications subscriptions (Figure 6.2.2) shows a peak in mobile phone subscriptions around 2013, followed by a gradual decline. Fixed line subscriptions remain stable but marginal. This saturation implies that access is no longer the issue—trust and meaningful engagement are. Voters are digitally reachable but emotionally disengaged. Opposition messaging must evolve from volume-based outreach to value-based signaling, where every message carries strategic weight.

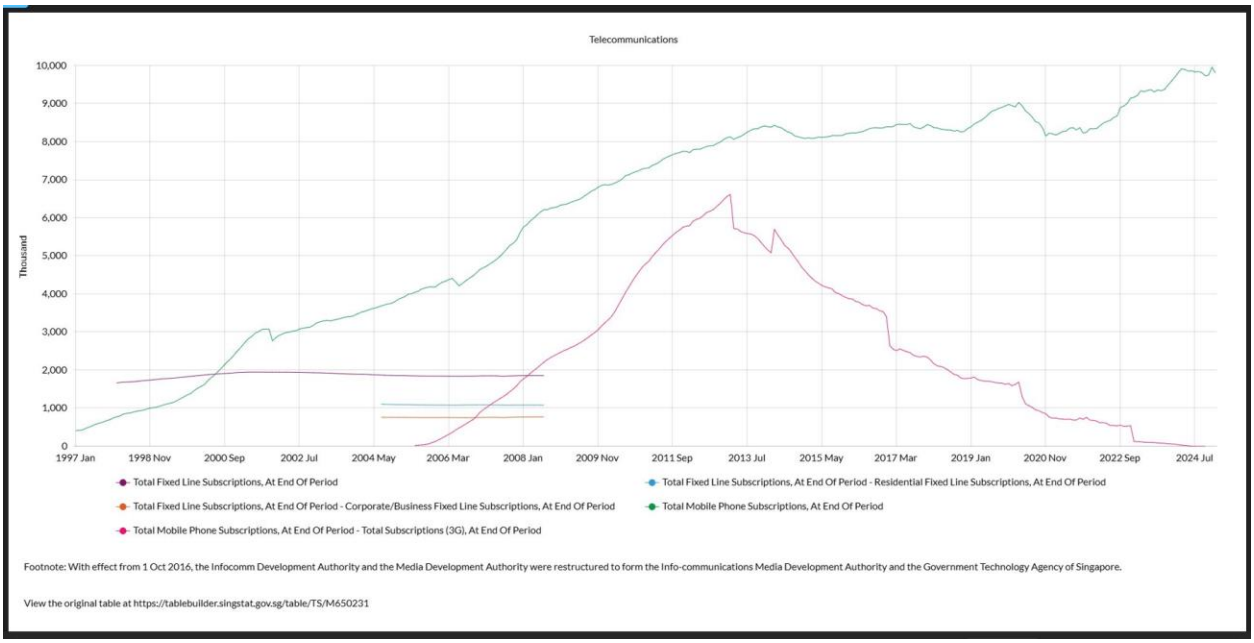

Figure 6.2.2 Telecommunication subscriptions (Source: Department of Statistics Singapore, 2025)

6.2.3 Business technology adoption: AI, e-payments and analytics

The graph on business usage of technologies (Figure 6.2.3) from 2017 to 2024 reveals:

1. Near-universal adoption of computers and internet
2. Rapid rise in e-payment systems
3. Steady growth in cloud computing and data analytics
4. A sharp uptick in artificial intelligence usage in 2024

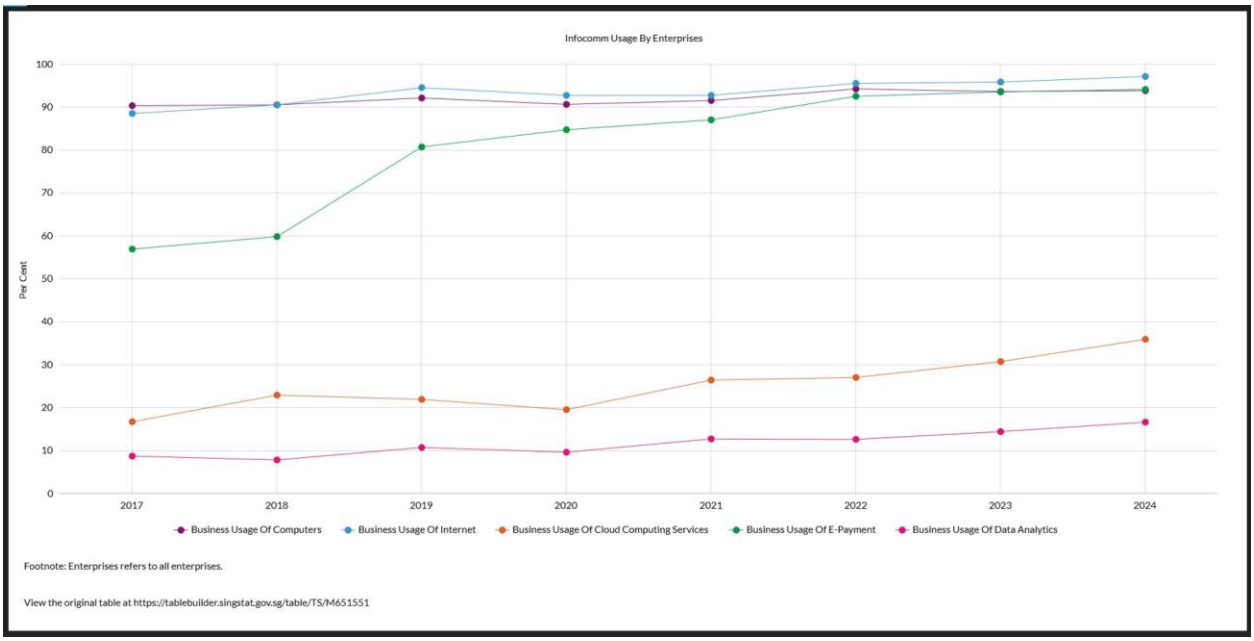

Figure 6.2.3 Business digital usage (Source: Department of Statistics Singapore, 2025)

These trends indicate that Singapore's business ecosystem is rapidly digitizing, with AI and analytics becoming mainstream. Opposition parties must respond by demonstrating policy fluency in emerging technologies, not just as economic tools but as governance instruments. The Firewall Leadership Model must now incorporate tech-policy signaling—where leaders articulate positions on AI ethics, data sovereignty and digital inclusion.

6.3 Final strategic insight

Opposition leadership in Singapore must evolve beyond reactive messaging and into strategic interface design—where emotional resonance, cybersecurity literacy and tech-policy fluency converge. The genotype–phenotype realignment is no longer optional; it is existential. In a digitally saturated, trust-fractured landscape, the opposition must become the firewall: resilient, transparent and strategically attuned to the anxieties and aspirations of a hyperconnected electorate.

References

Alford, J.R., Funk, C.L. and Hibbing, J.R. (2008) 'Are political orientations genetically transmitted', *American Political Science Review*, *102*(2), pp.233–248.

Braun, V., Clarke, V. and Gray, D. (2023) 'Innovations in thematic analysis: The role of AI and large language models', *Qualitative Research in Psychology*, *20*(1), pp.45–62

Channel NewsAsia (2025) 'Cybersecurity breaches in Singapore: UNC3886 espionage and Toppan ransomware incidents', [online] Available at: https://www.channelnewsasia.com

Department of Statistics Singapore (2025) *Crime cases recorded by category*. [dataset] Available at: https://data.gov.sg/dataset/crime-cases-recorded (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Employer tick mark media manpower by sector*. [dataset] Available at: https://www.tablebuilder.singstat.gov.sg (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Enterprise Infocomm Survey: Infocomm usage by enterprises*. [dataset] Available at: https://www.tablebuilder.singstat.gov.sg/table/TSM405511 (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Household access to internet by household composition*. [dataset] Available at: https://www.tablebuilder.singstat.gov.sg (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Individuals' key internet activities*. [dataset] Available at: https://public.tablebuilder.singstat.gov.sg/table/TS/M625051 (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Infocomm household survey: Households with computers*. [dataset] Available at: https://www.tablebuilder.singstat.gov.sg/table/TSM920351 (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Proportion of youth and adults with information and communications technology (ICT) skills, by age group and type of ICT skills*. [dataset] Available at: https://data.gov.sg/dataset/sdg-indicator-4-4-1 (Accessed: 18 September 2025)

Department of Statistics Singapore (2025) *Telecommunication subscription*. [dataset] Available at: https://data.gov.sg/dataset/telecommunication-subscription (Accessed: 18 September 2025)

Gandhi, J. and Lust-Okar, E. (2009) 'Elections under authoritarianism', *Annual Review of Political Science*, *12*, pp.403–422.

George, C. (2021) 'Singapore: The politics of regulated resilience', in Ong, T.T. and Postill, J. (eds.) *Digital political cultures in Southeast Asia*, Routledge, pp.45–67.

Hannan, M.T. and Freeman, J. (1984) 'Structural inertia and organizational change', *American Sociological Review*, *49*(2), pp.149–164.

Hartley, K. (2024) ‘Digital trust and democratic resilience: A Southeast Asian perspective’, *Journal of Digital Governance*, *6*(1), pp.12–29.
Infocomm Media Development Authority (2025) *Fixed internet broadband subscriptions per 100 population*. [dataset] Available at: https://data.gov.sg (Accessed: 18 September 2025)
Infocomm Media Development Authority (2025) *Telecommunication penetration rate*. [dataset] Available at: https://public.tableau.com/profile/imda (Accessed: 18 September 2025)
Levitsky, S. and Way, L.A. (2010) *Competitive authoritarianism: Hybrid regimes after the Cold War*, Cambridge University Press.
Lim, M. (2023) ‘Emotional publics and the politics of digital storytelling’, *Media, Culture & Society*, *45*(3), pp.487–504.
Mutalib, H. (2000) ‘Illiberal democracy and the future of opposition in Singapore’, *Third World Quarterly*, *21*(2), pp.313–342.
Newton Tech4Dev Network (2018) *Architects of networked disinformation: Behind the scenes of troll accounts and fake news production in the Philippines*, by Ong, J.C. and Cabañes, J.V.A.
Nye, J.S. (2022) ‘Cyber power and democratic legitimacy’, *Foreign Affairs*, *101*(4), pp.78–89.
Orgogozo, V., Morizot, B. and Martin, A. (2015) ‘The differential view of genotype–phenotype relationships’, *Frontiers in Genetics*, *6*, p.179.
Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T. and Tacchi, J. (2016) *Digital ethnography: Principles and practice*, SAGE Publications.
Postill, J. and Pink, S. (2012) ‘Social media ethnography: The digital researcher in a messy web’, *Media International Australia*, *145*(1), pp.123–134.
Tan, N. (2023) ‘Electoral engineering and opposition fragmentation in Singapore’, *Asian Journal of Political Science*, *31*(1), pp.1–20.
Tan, N. and George, C. (2022) ‘From protest to policy: Reframing opposition strategy in Southeast Asia’, *Journal of Democracy and Reform*, *14*(2), pp.56–74.
Tarrow, S. (1998) *Power in movement: Social movements and contentious politics*, 2nd ed., Cambridge University Press.
Teo, Y. (2024) ‘Trust in the age of encryption: Messaging platforms and political engagement in Singapore’, *Digital Asia Review*, *9*(1), pp.33–51.
The Diplomat (2024) ‘Singapore’s cybersecurity landscape: Strategic vulnerabilities and regional implications’, [online] Available at: https://thediplomat.com
Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, PublicAffairs