International Journal of Politics and Governance Issues
Volume 1, Issue 1, Mei 2026
E-ISSN : xxx-xxxx

Electoral Governance, Digital Disinformation, and Democratic Resilience: Comparative Institutional Analysis of Canada and Taiwan

Yuki Tanabe[1]

Yuki Tanabe

Graduate School of Law and Politics
University of Tokyo
Email: yuki.tanabe@u-tokyo.ac.jp

***Corresponding Author:** yuki.tanabe@u-tokyo.ac.jp

Citation: Aziz (2026). Electoral Governance, Digital Disinformation, and Democratic Resilience: Comparative Institutional Analysis of Canada and Taiwan (Book Antiqua 14pt Bold). *International Journal of Politics and Governance Issues*, *10*(4), xx–xx. https://doi.org/0000-0000

Published: 20/05/2026

ABSTRACT

Digital disinformation has become a central governance challenge for contemporary democracies, affecting electoral integrity, public trust, institutional legitimacy, and national security. This article examines how political institutions shape democratic resilience against digital disinformation through a comparative analysis of Canada and Taiwan. Both cases are liberal democratic systems with advanced digital infrastructures, competitive elections, and high exposure to foreign information influence. Yet their institutional responses differ significantly. Canada relies on an independent electoral management model, federal coordination, platform regulation, and public communication mechanisms, while Taiwan employs a whole-of-society resilience model integrating government agencies, civil society fact-checking networks, digital participation platforms, and cybersecurity institutions. Using comparative governance analysis and democratic resilience theory, this study argues that electoral resilience depends not only on legal regulation or technological monitoring but on institutional trust, civic capacity, public communication, and adaptive coordination among state and non-state actors. The findings indicate that Canada's model strengthens procedural neutrality and electoral administration credibility, whereas Taiwan's model demonstrates stronger societal mobilization and rapid disinformation response capacity. The article contributes to governance scholarship by linking electoral institutions, digital governance, public trust, democratic participation, and sustainable political resilience in an era of hybrid information conflict.

© 2025 by Author/s

Keywords: electoral governance; digital disinformation; democratic resilience; Canada; Taiwan; digital governance; public trust; cybersecurity; comparative politics; electoral integrity

INTRODUCTION

The integrity of democratic elections has become increasingly dependent on the ability of political institutions to govern digital information environments. Electoral competition now unfolds across social media platforms, encrypted messaging systems, algorithmic recommendation infrastructures, foreign influence operations, and rapidly circulating online narratives. While digital communication has expanded political participation and access to information, it has also intensified the circulation of disinformation, conspiracy narratives, coordinated manipulation, and synthetic media. These developments pose significant challenges for electoral governance, democratic legitimacy, and public trust.

The problem is not only technological but institutional. Disinformation becomes politically destabilizing when governance systems lack coordination, citizens distrust public institutions, electoral authorities cannot communicate effectively, or platform accountability remains weak. As democratic institutions worldwide confront polarization, declining trust, and foreign interference risks, electoral governance has become a central domain of democratic resilience. International IDEA has repeatedly warned that democratic institutions face growing pressure from misinformation, polarization, and weakened public confidence in elections (International IDEA, 2023, 2024). Similarly, OECD governance reports emphasize that trust, transparency, institutional communication, and digital governance capacity are essential to democratic resilience in digital societies (OECD, 2023).

Canada and Taiwan provide analytically important comparative cases. Both are democratic systems with advanced digital infrastructures, competitive electoral politics, and substantial exposure to digital influence operations. However, they differ in geopolitical threat environments, institutional coordination systems, public communication strategies, and civil society mobilization. Canada faces disinformation related to electoral interference, platform manipulation, domestic polarization, and foreign influence. Taiwan faces a more intense and continuous information threat environment due to its geopolitical position and sustained exposure to cross-strait influence operations.

Canada's electoral governance model is anchored in institutional neutrality, independent election administration, legal regulation of campaign finance and election communication, cybersecurity coordination, and federal democratic institutions. Elections Canada plays a central role in maintaining procedural credibility and public communication. The Canadian model emphasizes institutional independence and rule-based electoral administration.

Taiwan's model is more explicitly societal and adaptive. Its democratic resilience strategy integrates government agencies, civic technology networks, civil society fact-checkers, digital participation platforms,

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cybersecurity institutions, and rapid public communication mechanisms. Taiwan's experience demonstrates how democratic resilience can emerge through interaction between state capacity and civic mobilization.

Existing scholarship provides valuable foundations but remains incomplete. Electoral governance literature emphasizes electoral management bodies, campaign regulation, institutional neutrality, and electoral integrity (Norris, 2014). Digital governance literature examines platform accountability, algorithmic transparency, and state capacity (Mergel et al., 2023). Democratic resilience scholarship analyzes institutional trust, participation, polarization, and democratic backsliding (Levitsky & Ziblatt, 2018). Cyber governance research focuses on foreign interference, hybrid threats, and information security (DeNardis, 2020). However, these fields often remain analytically separated.

This article addresses five gaps. First, a theoretical gap persists concerning how electoral institutions mediate digital disinformation risks. Second, an empirical gap remains regarding how democracies build resilience across state and societal institutions. Third, a comparative gap exists because electoral disinformation studies often examine single cases without comparing institutional mechanisms. Fourth, a governance implementation gap concerns how public agencies, platforms, civil society, and citizens coordinate during elections. Fifth, a sustainability gap remains concerning how democracies sustain trust and legitimacy beyond immediate electoral cycles.

This study argues that democratic resilience against disinformation depends on four institutional capacities: credible electoral administration, adaptive digital governance, civic communication networks, and public trust. Where these capacities reinforce one another, democracies are more likely to resist manipulation without undermining freedom of expression. Where they are fragmented, disinformation governance may become reactive, politicized, or ineffective.

The analytical framework is:

Electoral Institutions → Digital Governance Coordination → Public Communication Capacity → Civic Trust → Democratic Resilience

The research objective is to analyze how Canada and Taiwan's contrasting governance systems shape institutional responses to digital disinformation and to explain their implications for electoral integrity, public trust, and democratic resilience..

METHODOLOGY

This study employs comparative governance analysis and democratic institutional analysis to examine how Canada and Taiwan respond to digital disinformation in electoral contexts. The cases were selected through a most-similar logic because both are advanced democracies with competitive elections, developed digital infrastructures, independent media ecosystems, and high public reliance on online political communication, yet they differ substantially in geopolitical exposure, institutional coordination models, civic technology ecosystems, and public communication

 © 2025 by Author/s

strategies. Canada represents an independent electoral administration model emphasizing legal neutrality, federal coordination, and procedural legitimacy, whereas Taiwan represents a whole-of-society resilience model emphasizing civic mobilization, rapid response, cybersecurity coordination, and participatory digital governance. The study analyzes five variables: electoral management capacity, digital governance coordination, cybersecurity preparedness, civil society participation, and public trust formation.

The empirical basis consists of triangulated evidence from electoral management reports, OECD digital governance assessments, International IDEA democracy reports, cybersecurity policy documents, public trust datasets, platform governance literature, and peer-reviewed studies on disinformation and democratic resilience. Comparative process tracing is used to identify causal mechanisms linking institutional arrangements to resilience outcomes, while interpretive institutional analysis evaluates how legal authority, public communication, civic participation, and cybersecurity coordination shape electoral governance. Reliability is strengthened through cross-source comparison between international reports, national policy documents, and academic literature. The study avoids fabricated interview data and does not attribute claims to unnamed respondents. Its main limitation is that disinformation threats evolve rapidly, especially with generative AI, meaning that findings should be interpreted as institutional trajectories rather than fixed institutional outcomes.

Findings and Discussion

1. Electoral Institutions and Procedural Legitimacy

Canada and Taiwan demonstrate that electoral legitimacy depends on institutional credibility before digital threats emerge. Canada's electoral governance relies heavily on the independence and professionalism of Elections Canada. This institutional design strengthens procedural legitimacy by insulating election administration from partisan control. Public communication about voting rules, foreign interference, and electoral security is centralized through formal institutional channels.

This model is particularly valuable in polarized information environments because independent electoral management bodies can serve as trusted arbiters of procedural facts. However, Canada's federal system also creates coordination complexity across national security agencies, provincial authorities, political parties, platforms, and civil society organizations. The strength of neutrality may therefore coexist with slower adaptive response.

Taiwan's electoral governance is shaped by a more acute threat environment. Its institutions must respond not only to routine campaign misinformation but also to sustained foreign influence operations. Taiwan's Central Election Commission works alongside cybersecurity agencies, civil society networks, media literacy organizations, and civic technology communities. This creates a broader resilience ecosystem.

The comparison reveals two pathways of electoral legitimacy. Canada emphasizes procedural neutrality, while Taiwan emphasizes adaptive societal resilience. Canada's model is institutionally credible but may be cautious. Taiwan's model is faster and more participatory but depends heavily on sustained civic mobilization.

The theoretical implication is that electoral governance should not be reduced to election-day administration. It is a continuous governance process involving institutional trust, information integrity, civic communication, and adaptive public authority.

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Digital Governance Coordination and Disinformation Response

Digital disinformation challenges conventional public administration because it moves rapidly across platforms, borders, and social networks. Effective governance therefore requires coordination across electoral institutions, cybersecurity agencies, communication regulators, platform companies, media organizations, and civil society.

Canada has developed coordination mechanisms to address election interference and online manipulation, including public communication protocols, cybersecurity monitoring, and platform engagement. Its approach is cautious and legally bounded, reflecting concerns about state overreach into political speech. This protects civil liberties but may limit rapid intervention against ambiguous influence campaigns.

Taiwan's digital governance system is more agile. Civic technology communities, government digital ministries, fact-checking organizations, and public communication teams coordinate rapidly to debunk false claims and circulate verified information. Taiwan's model shows how democratic societies can counter disinformation through transparency, humor, speed, and civic participation rather than censorship.

This comparison demonstrates that digital governance effectiveness depends on institutional speed and legitimacy. Slow responses allow disinformation narratives to become socially embedded. Overly coercive responses can undermine democratic freedoms. Taiwan's experience suggests that rapid civic-state collaboration can create a democratic alternative to both laissez-faire platform governance and authoritarian information control.

The findings support recent governance scholarship emphasizing adaptive administration and networked governance under conditions of uncertainty. Digital disinformation cannot be governed solely by law; it requires institutional ecosystems capable of rapid, credible, and publicly trusted response.

3. Public Trust, Civic Participation, and Democratic Resilience

Public trust is the central mediating variable between electoral governance and democratic resilience. Citizens are more likely to reject false information when they trust electoral institutions, public communication, media systems, and civic intermediaries.

Canada benefits from relatively strong institutional trust in electoral administration. Elections Canada's nonpartisan reputation supports public confidence in voting procedures. However, trust is uneven across social groups and vulnerable to politicized narratives imported from other democratic contexts. Disinformation concerning voting fraud, foreign influence, public health, immigration, and elite corruption can weaken confidence when institutional communication fails to reach fragmented audiences.

Taiwan's public trust model relies more heavily on civic participation and collective resilience. Civil society organizations, digital volunteers, and fact-checking groups play a major role in strengthening societal capacity to identify and resist manipulation. This model transforms citizens from passive recipients of official information into active participants in democratic defense.

© 2025 by Author/s

The comparison reveals that public trust is not produced only by institutional authority. It is co-produced through interaction between public agencies, civil society, media ecosystems, and citizens. Canada's model privileges institutional credibility; Taiwan's model privileges civic resilience. A more comprehensive theory of democratic resilience must integrate both.

The policy implication is that governments should invest in civic information infrastructure, media literacy, digital participation, and transparent communication rather than relying only on platform regulation or punitive laws.

---

4. Cybersecurity, Foreign Interference, and Institutional Adaptation

Foreign interference has become an increasingly important dimension of electoral governance. Cyberattacks, hacked materials, influence operations, bot networks, deepfakes, and coordinated harassment campaigns can disrupt electoral processes and public trust.

Canada's approach reflects national security coordination within democratic constraints. Intelligence agencies, electoral bodies, and public officials monitor threats while attempting to avoid politicizing security assessments. This restraint protects democratic neutrality but can produce public uncertainty when threats are disclosed ambiguously.

Taiwan faces more persistent cyber and information pressure. Its institutions have developed stronger routines for rapid public response, cybersecurity preparedness, and societal alertness. The Taiwanese case demonstrates that repeated exposure to digital threats can generate institutional learning and civic adaptation.

However, Taiwan's model also faces sustainability challenges. Continuous threat exposure can produce fatigue, politicization, or normalization of hostile information environments. Democratic resilience therefore requires not only crisis response but long-term institutional renewal.

The comparison shows that cybersecurity and electoral governance are increasingly inseparable. Election integrity now depends on protecting not only ballots and counting systems but also public information environments, institutional credibility, and civic trust.

Table 1. Analytical Matrix of Comparative Politics and Governance Development

Variable	Canada	Taiwan	Empirical Evidence	Analytical Interpretation
Electoral Governance Model	Independent electoral administration	Whole-of-society electoral resilience	Electoral commission reports; democracy indexes	Institutional credibility operates through different governance mechanisms
Digital Threat Environment	Foreign interference and domestic polarization	Sustained cross-strait influence operations	Cybersecurity and disinformation reports	Threat intensity shapes institutional adaptation
Governance	Federal and	Rapid civic-	OECD and	Coordinatio

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Coordination	legally bounded coordination	state coordination	national digital governance reports	n speed affects disinformation response capacity
Public Communication	Formal institutional communication	Distributed rapid response communication	Election information campaigns; fact-checking networks	Trust depends on both authority and civic reach
Civil Society Role	Supportive but less structurally embedded	Central to resilience ecosystem	Civic technology literature	Societal capacity mediates democratic resilience
Cybersecurity Integration	National security-electoral coordination	Integrated cyber-information resilience	Cyber governance documents	Electoral integrity increasingly depends on cybersecurity governance
Legitimacy Mechanism	Procedural neutrality	Participatory resilience and public mobilization	Public trust and participation datasets	Different democracies generate legitimacy through distinct pathways
Sustainability Implication	Stable but potentially slow adaptation	Adaptive but resource-intensive resilience	Institutional performance evidence	Long-term resilience requires institutional trust and civic renewal

The table demonstrates that electoral disinformation governance is shaped by institutional design, threat exposure, civic capacity, and public trust. Canada's strengths lie in procedural neutrality and independent administration. Taiwan's strengths lie in rapid adaptation and civic resilience. Both models reveal that democratic resilience requires more than regulation: it requires trusted institutions and active societies.

Theoretical Propositions

Proposition 1: Electoral resilience depends on the interaction between institutional credibility and digital governance capacity.

Independent electoral administration strengthens legitimacy, but it must be supported by adaptive digital response systems.

Proposition 2: Public trust mediates the effect of disinformation on democratic stability.

Disinformation is most damaging where citizens distrust electoral institutions, media systems, and public authorities.

Proposition 3: Civil society participation strengthens democratic resilience when connected to credible public

© 2025 by Author/s

institutions.

Civic fact-checking, digital participation, and media literacy are most effective when aligned with transparent institutional communication.

Proposition 4: Cybersecurity governance and electoral governance are now structurally interdependent. Election integrity requires protection of both technical infrastructure and public information ecosystems.

CONCLUSION

This article examined how Canada and Taiwan's governance systems shape institutional responses to digital disinformation and democratic resilience. The findings show that electoral governance in the digital age extends beyond formal election administration. It includes cybersecurity, public communication, platform governance, civic participation, and public trust.

Canada's model demonstrates the importance of independent electoral administration and procedural neutrality. These features strengthen institutional legitimacy and protect electoral governance from partisan manipulation. However, Canada's model may face challenges when digital threats require rapid, networked, and socially embedded responses. Taiwan's model demonstrates the value of whole-of-society resilience, civic technology, rapid fact-checking, and adaptive public communication. However, this model requires sustained civic energy and institutional coordination to remain effective over time.

The article contributes theoretically by linking electoral governance, digital governance, and democratic resilience. It shows that democratic resilience is not simply the absence of disinformation but the institutional and societal capacity to absorb, contest, and neutralize manipulation without undermining democratic freedoms.

Empirically, the comparison contributes evidence on how two democracies respond to digital threats under different geopolitical and institutional conditions. The findings suggest that resilient democracies require both credible electoral institutions and participatory information ecosystems.

The policy implications are clear. Governments should strengthen independent electoral management, transparent public communication, cybersecurity coordination, platform accountability, civic education, and civil society partnerships. Regulatory responses should avoid excessive censorship while ensuring that democratic institutions can respond effectively to manipulation.

The study is limited by the rapid evolution of generative AI and synthetic media, which may transform electoral disinformation in future cycles. Future research should examine how AI-generated content, automated influence operations, and platform governance reforms affect electoral resilience across different democratic systems.

Ultimately, this article argues that the future of democratic elections will depend on whether political institutions can combine procedural integrity, digital adaptability, civic trust, and democratic inclusion in an

Copyright © 2025 by Author/s. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

increasingly contested information environment.

REFERENCES

Ansell, C., Sørensen, E., & Torfing, J. (2021). The COVID-19 pandemic as a game changer for public administration and leadership. Public Management Review, 23(7), 949–960.

Bennett, W. L., & Livingston, S. (2020). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, 35(1), 3–20.

Bradshaw, S., & Howard, P. N. (2020). The global disinformation order. Computational Propaganda Research Project. Oxford Internet Institute.

DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press.

Elections Canada. (2023). Report on the 44th General Election. Elections Canada.

Freedom House. (2024). Freedom on the Net 2024. Freedom House.

Fukuyama, F. (2014). Political Order and Political Decay. Farrar, Straus and Giroux.

International IDEA. (2023). The Global State of Democracy 2023. International Institute for Democracy and Electoral Assistance.

International IDEA. (2024). The Global State of Democracy 2024. International Institute for Democracy and Electoral Assistance.

Levitsky, S., & Ziblatt, D. (2018). How Democracies Die. Crown.

Mergel, I., Ganapati, S., & Whitford, A. (2023). Agile governance capacity in the digital era. Government Information Quarterly, 40(1), 101759.

Norris, P. (2014). Why Electoral Integrity Matters. Cambridge University Press.

OECD. (2023). Building Trust and Reinforcing Democracy. OECD Publishing.

OECD. (2024). Facts Not Fakes: Tackling Disinformation, Strengthening Information Integrity. OECD Publishing.

Pierre, J., & Peters, B. G. (2020). Governance, Politics and the State (2nd ed.). Red Globe Press.

Reporters Without Borders. (2024). World Press Freedom Index 2024. RSF.

Taiwan Central Election Commission. (2024). Election Administration and Public Communication Report. Central Election Commission.

United Nations. (2023). World Public Sector Report 2023. United Nations Department of Economic and Social Affairs.

World Bank. (2024). GovTech Maturity Index 2024. World Bank.

World Economic Forum. (2024). Global Risks Report 2024. World Economic Forum.

 © 2025 by Author/s