

Article

From Formal Regulation to Operational Capacity: Asymmetric Adaptive Coordination in Deepfake Governance

Jing Shi^{1,*}

¹ College of Liberal Arts and Social Sciences, City University of Hong Kong, Hong Kong, China

* Correspondence: Jing Shi, College of Liberal Arts and Social Sciences, City University of Hong Kong, Hong Kong, China

Abstract: Deepfake governance is often approached as a problem of technical detection, legal prohibition, or platform responsibility. Yet formal regulation and multi-actor participation do not necessarily translate into effective governance capacity. This article examines why formally dense governance arrangements can remain operationally weak through a qualitative comparison of the Huangshi AI voice-impersonation case and the Cangnan AI face-swapping case. Drawing on publicly available police, judicial and procuratorial materials, regulatory documents, authoritative news reports, and platform or industry sources, the study combines structured-focused comparison with process tracing. The analysis identifies four interconnected mechanisms: temporal mismatch between technological change and institutional updating; jurisdictional fragmentation across the harm chain; regulatory dependence arising from capability and information asymmetries; and incentive divergence that makes collaboration selective and episodic. The findings show that governance weakness arises not simply from the absence of rules or actors, but from failures to convert dispersed information into timely, verifiable, and coordinated action and to translate case responses into institutional learning. The article develops asymmetric adaptive coordination as a mechanism linking technological turbulence, distributed authority, unequal information control, and divergent incentives. It argues that effective deepfake governance depends less on adding rules or participants than on building capacities for timely coordination, auditability, learning, and correction while safeguarding security, privacy, due process, innovation, and public trust.

Keywords: deepfakes; AI governance; adaptive coordination; collaborative governance; operational capacity; public value

1. Introduction

Deepfakes are synthetic or substantially manipulated audio, images, video, or other digital content that represent a person, event, or interaction as if it were authentic. The technology has legitimate uses in film production, accessibility, education, cultural expression, and creative work. Governance problems arise when synthetic media are used without authorization to impersonate identity, induce reliance, invade privacy, manipulate public communication, or facilitate fraud. The relevant object of governance is therefore not synthetic content in isolation, but the relationship between its production and circulation, the actors who use it, the contexts in which it is encountered, the harms it produces, and the institutions responsible for responding.

Deepfakes are especially difficult to govern because they appropriate the ordinary cues through which people establish identity and trust. A familiar voice can make an urgent request appear to come from a relative; a synthetic face can make a remote actor appear to be an authorized account holder. In such cases, the problem is not simply that false content exists. The evidentiary signals on which victims, platforms, financial institutions, and frontline officials ordinarily rely have themselves become part of the deceptive process. Research has accordingly linked deepfakes to privacy invasion,

Received: 19 July 2026

Revised: 02 September 2026

Accepted: 15 September 2026

Published: 21 September 2026



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

political manipulation, discrimination, reputational harm, fraud, and the declining reliability of audiovisual evidence [1-4].

These risks have generated substantial regulatory responses. China, for example, has established rules governing deep synthesis services, generative AI services, and the labeling of AI-generated or synthetic content [5-7]. These measures operate alongside criminal law, personal information protection, cybersecurity regulation, financial risk control, telecommunications administration, and platform self-governance. Public security organs, cyberspace regulators, telecommunications operators, financial institutions, content platforms, technical providers, and users may therefore all participate in the response to deepfake-related harms. Deepfake governance is, in this sense, neither institutionally empty nor dependent on a single actor.

This institutional density creates a more specific governance puzzle. Formal regulation, assigned responsibilities, and multi-actor participation do not necessarily translate into effective operational capacity. Rules may exist without producing timely verification; relevant information may be distributed across organizations that cannot readily combine it; authorities with legal powers may depend on platforms or technical providers for the data and expertise needed to act; and cooperation may intensify after visible incidents without becoming a routine capacity for prevention and learning. The central question of this article is therefore not simply whether deepfakes are regulated, but why formally dense governance arrangements can remain operationally weak. More specifically, it asks how information, authority, technical capability, and organizational incentives interact across the response chain, and under what conditions participation is converted into governance capacity.

The article investigates this question through a qualitative comparison of two Chinese cases. The Huangshi case concerns AI-assisted voice impersonation in a family fraud scenario involving older victims. It makes visible the temporal gap between real-time social engineering, identity verification, reporting, and technical confirmation. The Cangnan case concerns the use of AI face-swapping in a theft-related chain involving identity verification and account or platform controls. It reveals how personal information, synthetic identity signals, authentication systems, financial processes, and subsequent intervention may be distributed across different organizations. The cases differ in modality and operational setting, but both allow examination of the same underlying question: why the presence of rules and relevant actors does not by itself ensure that information is converted into timely and coordinated action.

The article makes three related contributions. First, it shifts the analytical focus from the formal presence of governance arrangements to their operational capacity. The effectiveness of deepfake governance cannot be inferred from the existence of rules, participating organizations, removed content, or solved cases alone. It also depends on whether the governance system can detect emerging risks in time, preserve and exchange usable evidence, coordinate intervention across organizational boundaries, trace responsibility, provide relief, and learn from previous cases. Second, the article develops the concept of asymmetric adaptive coordination to explain how technological turbulence interacts with distributed authority and unequal control over information, expertise, and intervention capacity. Environmental turbulence helps explain why governance must adapt, while collaborative governance explains why interorganizational cooperation is necessary. Their combination, however, does not by itself explain how coordination operates when the participating actors possess different forms and degrees of capacity. Asymmetric adaptive coordination identifies this organizational problem and the mechanisms through which it affects governance outcomes. Third, the article treats public values as boundary conditions of adaptive coordination. Faster and more integrated intervention may improve security, but it can also increase privacy intrusion, false positives, procedural unfairness, restrictions on legitimate expression, or distrust when safeguards for proportionality, explanation, and correction are absent.

The argument proceeds as follows. Section 2 reviews research on deepfake governance and develops the theoretical framework of asymmetric adaptive coordination.

Section 3 explains case selection, data sources, comparative strategy, process tracing, coding, and validity safeguards. Section 4 identifies four mechanisms through which formal governance arrangements can remain operationally weak: temporal mismatch, jurisdictional fragmentation, regulatory dependence and capability asymmetry, and incentive divergence. Section 5 develops the theoretical implications of these mechanisms and examines the public-value boundaries of adaptive coordination. Section 6 concludes by specifying the conditions under which multi-actor participation can be converted into durable governance capacity.

2. Deepfake Governance and the Limits of Existing Explanations

2.1. From Technical Detection to Governance

Research on deepfakes has developed along several partially connected lines. The first is technical, examining how synthetic media are generated and how detection, provenance, watermarking, metadata, and source authentication may support verification. This work is indispensable because governance cannot operate without some capacity to identify or contextualize manipulated content. Yet detection alone does not constitute governance. A detector may indicate that a file is likely to have been manipulated without identifying who created or distributed it, which institution can intervene, what evidence can be preserved, who should receive assistance, or what response is proportionate. Detection systems also operate within an adversarial cycle in which advances in generation alter the data and assumptions on which existing detection methods depend [8, 9].

A second line is legal and regulatory. Legal scholarship has mapped harms associated with deepfakes, including privacy invasion, identity impersonation, non-consensual sexual imagery, defamation, electoral manipulation, national security risks, and the erosion of the evidentiary value of recordings [1, 2]. Regulatory approaches have increasingly moved beyond a single prohibition toward layered obligations involving providers, deployers, distributors, and platforms. Chinese rules governing deep synthesis, generative AI services, and synthetic-content labeling illustrate this shift toward *ex ante* duties, technical labeling, security management, and platform responsibility [5-7]. Such rules specify what actors should do, but their existence does not by itself explain how formal duties become timely and coordinated responses in particular incidents.

A third line focuses on platforms and content moderation. Research on platform governance shows that moderation combines private ordering with increasingly public functions. Platforms use automated systems, human review, user reports, terms of service, and escalation procedures to shape visibility and access, while public authorities increasingly depend on platforms for monitoring, evidence, and enforcement support [10-12]. This literature demonstrates that platform rules are not merely technical instruments: they define categories of harm, allocate attention, and determine which signals become visible to other actors. It also identifies recurrent problems of opacity, uneven error, limited explanation, and the tendency to optimize measurable outputs rather than the broader public value of governance decisions.

A fourth line examines the social, epistemic, and democratic consequences of synthetic media. Deepfakes need not successfully deceive every viewer to generate harm. They can increase uncertainty about authenticity and weaken confidence in news, institutions, and recorded evidence [3, 4]. The related "liar's dividend" describes the possibility that the known manipulability of audio and video allows authentic evidence to be dismissed as fabricated [1]. This literature therefore extends the analysis beyond direct individual loss to public trust, verification costs, reliance on digital services, and unequal vulnerability to deception.

A fifth line locates deepfake abuse within cybercrime and transnational illicit economies. It emphasizes the division of labor among data brokers, tool providers, social-engineering teams, account operators, payment intermediaries, and money launderers, as well as the difficulty of responding to chains that cross institutional and territorial

boundaries [13, 14]. This perspective makes the operational chain visible, but it often remains analytically separated from work on platform governance and public administration.

Taken together, these literatures explain important dimensions of the problem: technical vulnerability, legal obligation, platform control, public trust, and criminal organization. What remains less clear is how these dimensions interact once regulation and multiple responsible actors are already present. The relevant question is not only whether a synthetic signal can be detected or whether a legal rule applies, but whether information can reach the actor capable of acting, whether it can be verified and used in time, whether interventions can be coordinated across organizational boundaries, and whether individual responses generate learning for subsequent cases. The analytical problem is therefore the conversion of formal and distributed governance resources into operational capacity.

2.2. Regulatory Adaptation under Technological Turbulence

The organizational environment perspective begins from the premise that public organizations do not operate within stable external conditions. Thompson, Zald, and Scott [15] emphasize organizational dependence on actors and resources beyond formal boundaries, while Burns and Stalker [16] distinguish rigid, rule-centered arrangements from more adaptive organizational forms. Applied to deepfakes, technological turbulence refers not simply to rapid technical change, but to the uncertainty, cross-domain effects, and limited visibility that accompany changing forms of synthetic media.

Four features are particularly important. First, the production and circulation of synthetic content may change faster than formal rules, training materials, procurement cycles, and frontline routines. Second, harmful applications are difficult to predict because the same tools can be repurposed across fraud, impersonation, harassment, political communication, and account compromise. Third, a single incident may cross content, telecommunications, finance, personal data, and criminal-justice domains. Fourth, information required for intervention is often distributed across organizations. A victim may encounter a suspicious voice but possess no technical evidence; a platform may possess interaction logs but lack the wider fraud context; and a public-security body may possess investigative authority without direct access to relevant platform or model data.

Regulatory adaptation consequently involves more than revising formal rules when a new technology appears. It requires an ongoing cycle of sensing, interpretation, response, and learning. Sensing concerns the identification of emerging tools, attack patterns, and victimization contexts. Interpretation converts dispersed signals into categories that can be understood across organizational boundaries. Response translates that understanding into warning, evidence preservation, temporary safeguards, or proportionate intervention. Learning feeds experience from individual cases into rules, operating procedures, platform controls, training, and public guidance. Where one of these links breaks, an organization may identify a problem without being able to classify it, classify it without being able to intervene, or intervene without generating knowledge for subsequent cases [17].

Institutional lag is therefore relational rather than merely chronological. A formally valid rule may have limited operational effect when it is not connected to current risk categories, responsible units, information-access procedures, evidence standards, or review cycles. Conversely, an effective technical control within a platform may fail to protect users if its signals cannot be connected to police reporting, financial intervention, victim assistance, or subsequent review. The relevant analytical unit is thus the governance cycle through which changing risks are recognized, interpreted, acted upon, and learned from, rather than the legal rule or technical instrument considered in isolation.

2.3. Interorganizational Dependence and Collaborative Governance

Collaborative and network governance perspectives explain why complex public problems cannot ordinarily be managed by a single organization. Wicked problems exceed the knowledge, authority, and resources of individual institutions, making

governance dependent on exchanges of information, expertise, legitimacy, and operational capacity across organizational boundaries [18-20]. Deepfake-related incidents illustrate this interdependence. Public-security organs may contribute investigative authority and case knowledge; platforms may control logs, account information, content signals, and technical assessments; financial institutions may provide transaction monitoring and emergency controls; communications operators may hold routing or account-related evidence; regulators may establish standards and escalation procedures; and users may provide the initial report and contextual information needed to interpret suspicious activity.

The existence of multiple actors, however, should not be equated with effective collaboration. Ansell and Gash [21] conceptualize collaborative governance as a process involving dialogue, trust building, commitment, shared understanding, and intermediate outcomes. Relational-governance research similarly suggests that formal safeguards and trust can operate as complements rather than substitutes: formal arrangements establish obligations and accountability, while repeated interaction enables organizations to address contingencies that cannot be fully specified in advance [22, 23].

Deepfake governance adds a further complication because interdependence is accompanied by substantial asymmetries in information and capability. Platforms and technical providers may control the data, interfaces, technical knowledge, and operational timelines required by regulators and investigators. Public authorities may possess legal powers while lacking equivalent visibility into technical systems. Victims and users occupy an even weaker position: they may have to make immediate judgments about authenticity while possessing few independent means of verification or of challenging an automated determination. Interorganizational cooperation can therefore coexist with dependence, and formal participation can coexist with limited accountability.

The participating actors also face different incentives. Public agencies seek security, lawful procedure, victim protection, and institutional legitimacy. Platforms must balance safety against service continuity, user growth, privacy obligations, innovation, engineering costs, and liability. Financial institutions seek to reduce fraud while limiting false positives and disruption to legitimate customers. Users seek both rapid protection and fair treatment. Because the costs and benefits of information exchange are distributed unevenly, actors may cooperate intensively after highly visible incidents while investing less in routine data exchange, shared classifications, joint testing, and preventive learning. The analytical problem is therefore not simply whether cooperation occurs, but whether interorganizational dependence is organized in a way that converts dispersed resources into sustained operational capacity.

2.4. Asymmetric Adaptive Coordination: Linking Adaptation and Interorganizational Dependence

The two perspectives identify complementary dimensions of deepfake governance. The organizational-environment perspective explains why rapidly changing risks place pressure on fixed rules and established routines. Collaborative governance explains why responding to such risks requires the exchange of information and resources across organizational boundaries. Neither perspective alone, however, fully specifies how adaptation and collaboration operate when authority, information, expertise, and intervention capacity are distributed unevenly among the participating actors.

This article conceptualizes that problem as asymmetric adaptive coordination. Asymmetric adaptive coordination refers to the organizational capacity to align changing technical signals, distributed authority, unequal information and expertise, and divergent incentives around a time-sensitive public problem. The concept has three defining features. It is adaptive because governance must revise its understanding and response as technologies and harmful uses change. It is coordinative because effective action depends on sequences of interdependent decisions and handoffs rather than on a single organization. It is asymmetric because the actors involved possess different forms and degrees of information, expertise, authority, and intervention capacity.

The framework therefore treats governance outcomes as the product of several interacting conditions rather than of a single deficiency. Technological turbulence creates pressure for continuous adaptation. Distributed authority makes interorganizational coordination necessary. Unequal control over information, expertise, and intervention capacity conditions how that coordination operates, while divergent incentives affect its continuity and scope. Together, these conditions can produce four observable mechanisms: temporal mismatch between technological change and institutional updating; jurisdictional fragmentation across the harm chain; regulatory dependence and capability asymmetry between public authorities and technical actors; and incentive divergence, which makes collaboration selective or episodic.

These mechanisms affect whether governance resources are converted into operational capacity. Temporal mismatch can delay recognition and intervention. Jurisdictional fragmentation can disrupt handoffs and obscure responsibility. Capability asymmetry can reduce the independent verifiability of technical claims. Incentive divergence can weaken prevention and institutional learning. Their consequences extend beyond immediate security outcomes to privacy, procedural fairness, public trust, victim relief, and the risk of excessive intervention against legitimate synthetic expression.

Adaptive coordination capacity can mitigate these problems when governance arrangements create shared problem representations, assign responsibility for interorganizational handoffs, establish time-bound and lawful information exchange, make technical claims auditable, and connect case outcomes to subsequent rules and organizational practice. The purpose of coordination is therefore not to eliminate organizational differences, but to make those differences governable (As shown in Table 1).

Table 1. Analytical Framework for Asymmetric Adaptive Coordination

Analytical element	What to observe	Failure mechanism	Likely consequence
Technological turbulence	New tools, changing attack vectors, uncertain signals, rapid circulation	Institutional updating cannot keep pace with the changing object of regulation	Delayed recognition and improvised response
Distributed authority	Multiple departments and firms own different steps in the fraud chain	No actor owns the full chain or the handoff between steps	Jurisdictional gaps and responsibility ambiguity
Capability asymmetry	Unequal access to data, models, logs, expertise, and evidence	Regulators depend on the regulated or technical partner to define the facts	Low verifiability and weak accountability
Divergent incentives	Different costs, benefits, liability risks, and performance metrics	Cooperation is selective, episodic, or symbolic	Weak prevention and limited institutional learning
Adaptive coordination capacity	Shared categories, lead agency, protocols, audits, feedback, appeal	Coordination converts information into timely and proportionate action	More resilient governance and protection of public values

The framework therefore shifts the analytical question from whether rules and participating actors exist to whether their distributed resources can be combined at the points where a risk must be recognized, interpreted, verified, interrupted, and learned from. This distinction provides the basis for the comparative analysis that follows.

3. Research Design and Methods

3.1. Case Selection

The study uses two information-rich cases selected for analytical contrast rather than statistical representativeness. Both cases involve harmful uses of synthetic identity signals and occurred within a regulatory environment in which responsibilities for fraud prevention, platform governance, personal information protection, telecommunications, and digital-content management were formally distributed across public and private actors. At the same time, the cases differ in modality, interaction structure, and the point at which the victim encounters the manipulated identity signal. The Huangshi case centers on AI-assisted voice impersonation and urgent interpersonal persuasion, whereas the Cangnan case centers on AI face-swapping, identity verification, and a more distributed theft-related chain involving both digital and offline links.

The paired design serves three analytical purposes. First, it reduces the risk that the proposed explanation merely reflects the technical characteristics of one modality. If similar organizational mechanisms are observable in both a real-time voice-fraud case and a visual identity-verification case, they are more plausibly associated with governance arrangements than with the technical medium alone. Second, the contrast allows the analysis to examine how a common governance problem appears differently across operational settings. Temporal mismatch, for example, may arise as an immediate verification problem in a real-time call but as a control, evidence, and handoff problem in an identity or account chain. Third, the cases permit comparison between the formal presence of responsible actors and the operational capacity produced by their interaction: who possessed relevant information, who had authority to act, how responsibilities were distributed, and whether information crossed organizational boundaries within the available intervention window.

The unit of analysis is the governance episode surrounding the harmful use of synthetic identity signals rather than the individual offender or isolated media artifact. Each episode is reconstructed as a sequence extending, where evidence permits, from data or tool access and preparation of the synthetic signal to victim contact or authentication, detection, reporting, evidence preservation, interorganizational handoff, intervention, investigation or adjudication, and subsequent institutional learning. Claims about technical details are limited to what can be established from the public record. Where a stage cannot be observed, it is treated as evidentially unavailable rather than inferred from the proposed framework.

Because the article examines whether formal governance arrangements were converted into operational capacity, the temporal relationship between each case and the applicable regulatory framework is also treated as part of the case context. Only rules and formal obligations in force or otherwise demonstrably applicable at the relevant time are used to characterize the institutional environment of a case.

3.2. Data Sources

The empirical corpus consists entirely of publicly available materials. Sources were organized by evidentiary function so that no single institutional account determined the reconstruction of either case (As shown in Table 2).

Table 2. Public Evidence Sources and Their Analytical Use

Source category	Examples of material	Analytical use and safeguard
Police reports	Public police briefings, case alerts, investigative summaries, public safety reminders	Reconstruct reported events, victim contact, investigative triggers, and the limits of publicly disclosed technical facts
Court and procuratorate materials	Judgments, indictments, non prosecution decisions,	Check legally established facts, evidence categories, procedural outcomes, and victim relief;

	procuratorate case explanations	distinguish adjudicated facts from media description
Government regulatory documents	Deep synthesis rules, generative AI measures, labeling rules, cybersecurity and personal information guidance	Map formal duties, assigned responsibilities, reporting and labeling expectations, and the institutional update context
Authoritative news reports	Reports by national or provincial public media and official news organizations	Track chronology, public framing, official warnings, and facts not available in legal documents; cross check with primary materials where possible
Platform and industry documents	Terms of service, safety policies, transparency materials, technical or industry guidance	Identify platform controls, reporting channels, moderation assumptions, and the incentives and limits surrounding cooperation

The source types perform different evidentiary functions. Police, judicial, and procuratorial materials are treated as stronger evidence for reported events and legally established facts. Regulatory documents are used to identify formal institutional design and applicable obligations, not to infer successful implementation. News reports are used principally to reconstruct chronology and public descriptions of the cases. Platform and industry documents are used to identify stated practices and available technical or organizational controls, but claims about their effectiveness require independent corroboration.

The evidence corpus was assembled around the two cases and the regulatory arrangements relevant to the governance stages identified above. Materials were retained when they contributed directly to the chronology of a case, established the role or authority of an actor, documented an organizational relation, identified an applicable rule or control, or provided evidence relevant to one of the proposed governance mechanisms. Materials that merely repeated previously established descriptions without adding factual or institutional information were not treated as independent corroboration.

3.3. Analytical Procedure

The comparison follows the logic of structured-focused comparison. The same analytical questions were applied to both cases: What changed in the technological or criminal environment? Which actors entered the episode, and what information, authority, or technical capacity did each control? Where did relevant information first become available, and where did it cease to travel? Which organization possessed the authority or capability to intervene at each stage? What shaped the timing and scope of cooperation? What response followed, and what effects did it have on security, privacy, trust, due process, or victim relief? Applying a common set of questions preserves comparability while allowing differences between the cases to remain visible [24].

Within each case, process tracing was used to reconstruct the sequence linking governance conditions to operational outcomes [25, 26]. The analysis examined, where observable, data or tool access; preparation of the synthetic identity signal; contact with the victim or platform; the point of reliance or authentication; detection or reporting; evidence preservation; interorganizational handoff; intervention; investigation or adjudication; and post-case learning. Process tracing is not used here to claim access to every hidden action of an offender or organization. Its purpose is to assess whether the public record supports the proposed links between organizational conditions and changes in the timing, quality, or direction of the response.

Causal claims are therefore mechanism-oriented and evidence-bounded. A mechanism is treated as supported when the public record establishes both the relevant governance condition and its connection to an observable consequence in the response

sequence. A finding of information dependence, for example, requires evidence not merely that a platform participated, but that another actor required information or technical capacity controlled by that platform and that this dependence affected verification, intervention, or accountability. Similar standards are applied to temporal mismatch, jurisdictional fragmentation, capability asymmetry, and incentive divergence.

Alternative explanations were considered throughout the reconstruction. In particular, the analysis examined whether observed weakness could be explained more parsimoniously by the absence of an applicable rule, an isolated technical failure, individual error, or lack of participation by a relevant actor. Where the public evidence cannot distinguish among competing explanations, the article does not treat the proposed mechanism as established.

3.4. Coding and Evidence Evaluation

The coding framework combines theory-guided and evidence-sensitive categories. Initial dimensions were derived from the research question and the theoretical framework, but coding remained open to case information that did not fit the expected mechanisms. The purpose of coding was not to classify every observation as evidence of asymmetric adaptive coordination, but to distinguish descriptive facts from relational conditions, proposed mechanisms, and governance outcomes.

Coding was conducted at the level of an event, organizational relation, or governance response. Four types of codes were distinguished. Descriptive codes recorded what occurred and when. Relational codes identified which actor controlled relevant information, expertise, authority, or intervention capacity. Mechanism codes captured whether and how an observed condition contributed to delay, fragmentation, dependence, or selective cooperation. Outcome codes recorded consequences for operational capacity and public values, including security, privacy, trust, due process, expression, innovation, and access to remedy (As shown in Table 3).

Table 3. Coding Dimensions

Coding dimension	Core question	Indicative evidence
Technological change	What changed in the tool, modality, accessibility, or attack pattern?	Voice cloning, face changing, identity signal manipulation, tool circulation, new use context
Actor configuration	Which public, private, and social actors participated, and what role did each play?	Police, regulators, platforms, financial institutions, communication operators, victims, users
Information dependency	Who needed information or expertise controlled by another actor?	Logs, account data, technical assessments, transaction signals, evidence preservation
Jurisdictional fragmentation	Where were responsibilities divided across departments, sectors, or territories?	Handoffs, overlapping mandates, cross platform or cross border links, unclear lead responsibility
Incentive structure	What costs and benefits shaped the willingness and timing of cooperation?	Compliance cost, false positive risk, liability, reputation, public safety, victim relief
Governance response	What was done, when, by whom, and through which instrument?	Warning, blocking, labeling, investigation, evidence exchange, emergency control, prosecution
Public value consequences	What values were protected, weakened, or traded off?	Security, privacy, trust, due process, expression, innovation, access to remedy

Evidence evaluation followed a convergence rule. A factual claim was retained when it was directly established by a primary or official source or when independent public

sources converged without material contradiction. A mechanism claim required evidence establishing both the relevant organizational relation and its observable effect on the response sequence. Where possible, mechanism claims were supported by more than one type of source. Repetition of the same originating account across multiple news reports was not treated as independent corroboration.

The analysis also distinguishes absence of evidence from evidence of absence. Where the public record does not disclose a technical process, organizational exchange, or internal decision, the analysis does not infer that it did not occur. Qualified formulations such as "the public record indicates," "the available materials document," or "the case is consistent with" are used where the evidence supports a plausible but incomplete inference.

3.5. Validity and Limitations

The study relies exclusively on publicly available materials and therefore does not claim access to confidential investigation files, internal platform data, proprietary model parameters, regulatory correspondence, or interviews with victims, officials, or platform personnel. This limits the ability to observe informal negotiations, undisclosed technical controls, unsuccessful interventions, and internal organizational learning that never entered the public record.

Several safeguards were used to reduce these limitations. First, different source types were cross-checked rather than treated as interchangeable. Public-security and media accounts were compared with judicial or procuratorial materials where available; formal rules were compared with the roles and response sequences documented in the cases; and platform statements were treated as accounts of stated practice rather than independent evidence of effectiveness. Second, the analysis distinguishes directly documented facts from theoretically informed inference. Third, alternative explanations were considered before a mechanism was attributed to a case. Fourth, technical details were not reconstructed beyond what the source record could establish. The analysis therefore does not identify a particular model, algorithmic bypass, data-acquisition route, or internal platform process unless supported by the available evidence.

The findings are intended as analytical rather than statistical generalization. Two cases cannot establish how frequently the identified mechanisms occur across deepfake incidents, platforms, or jurisdictions. They can show how particular mechanisms operate under specified conditions and generate propositions that may be examined in additional cases. The public nature of the evidence also introduces selection and reporting bias: highly visible incidents are more likely to be documented, while routine preventive interventions, unsuccessful reports, and internal coordination may remain invisible. These limitations narrow the scope of the claims, but they do not prevent the cases from being used to examine how formally established governance arrangements are, or are not, converted into operational capacity.

4. Findings

The comparative analysis identifies four mechanisms through which formally established governance arrangements can remain operationally weak: temporal mismatch, jurisdictional fragmentation, regulatory dependence and capability asymmetry, and incentive divergence. These mechanisms do not imply that regulation or cooperation is absent. Rather, they concern the points at which formal rules, distributed information, and organizational participation fail to become timely and usable governance capacity.

4.1. Temporal Mismatch between Technological Change and Institutional Response

The first mechanism concerns the different speeds at which harmful uses of synthetic media and institutional responses operate. In the Huangshi case, AI-assisted voice impersonation was embedded in an ordinary interpersonal communication setting. The reported interaction relied on a recognizable voice, an urgent request, and a short decision window. The operational problem therefore arose before any formal technical determination of whether the voice was synthetic could realistically be completed. Rules

addressing fraud or impersonation provided a basis for subsequent intervention, but did not by themselves create an immediate verification mechanism at the point at which the victim was required to decide whether to trust the caller.

The sequence illustrates a temporal asymmetry between exposure and verification. The deceptive interaction could occur immediately, whereas identity confirmation, reporting, transaction intervention, investigation, and technical examination required successive organizational steps. The public record therefore indicates a gap between the time at which reliance occurred and the time at which institutions could establish and act upon the relevant facts. The problem was not necessarily the absence of an applicable rule, but the difficulty of translating that rule into action within the available intervention window.

The Cangnan case shows a related problem in a more distributed setting. The reported use of AI face-swapping intersected with identity verification and subsequent account or property-related processes. Here, temporal mismatch did not arise primarily from a single real-time conversation. It arose from the movement of a synthetic identity signal across several technical and organizational stages before the wider significance of the event could be reconstructed. Controls at individual points could address authentication, account activity, or subsequent investigation, but those controls did not necessarily operate on the same temporal cycle or with a shared representation of the emerging risk.

Across the two cases, temporal mismatch therefore refers to the distance between the speed at which a harmful use becomes actionable and the speed at which institutions can recognize, verify, classify, and respond to it. Technological change matters not simply because it produces new tools, but because it changes the point in the sequence at which effective intervention must occur. Operational weakness emerges when institutional updating remains concentrated in formal rules or post-incident response while the relevant risk has shifted to an earlier stage of interaction or authentication.

4.2. Jurisdictional Fragmentation Across the Fraud Chain

The second mechanism concerns the distribution of responsibility across a harm chain that extends beyond the boundaries of any single organization. Deepfake-enabled incidents may involve different stages of data access, synthetic-content production, communication or authentication, account activity, payment or property transfer, reporting, investigation, and evidence preservation. These stages correspond to different organizational competences and sources of information.

In the Huangshi case, the victim encountered the harm locally through an interpersonal communication, but investigation and possible intervention depended on information distributed beyond that immediate interaction. The victim could report the incident but could not independently reconstruct the communication, financial, or technical chain. Public-security authorities possessed investigative powers, while other actors could hold transaction, communication, or contextual information relevant to verifying the event. The operational problem therefore extended beyond the initial report to the transfer and combination of information held by different actors.

The Cangnan case makes this fragmentation more visible because the synthetic identity signal intersected with an authentication or account process. Information concerning the manipulated identity, the authentication event, subsequent account activity, and later realization of the harm could be distributed among different organizations. No single actor necessarily possessed the complete sequence at the point when its own part of the event became visible. An authentication anomaly, for example, could have a different meaning when viewed in isolation than when linked to subsequent account or property activity.

The comparative pattern is therefore not merely one of organizational specialization. Specialization becomes fragmentation when the meaning of a signal depends on information held elsewhere and the handoff between organizations does not preserve that context. In both cases, the governance episode extended across institutional boundaries

while formal responsibilities remained divided by sector, function, or stage of response. Operational weakness arose at the interfaces between those responsibilities rather than from the complete absence of responsible actors.

4.3. Regulatory Dependence and Capability Asymmetry

The third mechanism concerns unequal access to the information and technical capacity required to establish what occurred. Public authorities may possess legal powers to investigate or intervene while relevant operational data, technical assessments, or system-level information are controlled by platforms, communications operators, financial institutions, or other technical actors. Formal authority and factual visibility are therefore not necessarily located in the same organization.

In the Huangshi case, the victim's report could establish the experience of receiving a familiar-sounding voice and an urgent request, but determining the technical status of the communication required forms of evidence that were not available to the victim alone. Communication records, digital traces, and technical assessment could therefore become necessary for moving from a reported experience to an evidentially usable account. The case illustrates a distinction between possessing contextual knowledge of harm and possessing the technical means to verify how that harm was produced.

The Cangnan case reveals a related asymmetry around identity verification. Authentication systems are operated through technical configurations, logs, thresholds, and internal decision procedures that are not ordinarily visible to outside users and may not be immediately visible to public authorities. When a synthetic identity signal passes through such a system, reconstruction of the event depends partly on information generated and retained by the organization operating that system. The same organization may therefore be both part of the governance response and an important source of evidence about the performance of its own controls.

This asymmetry affects more than access to raw data. It also affects how incidents are categorized. The same event may be represented as an authentication anomaly, an account-security problem, a fraud incident, or a synthetic-media problem, and each description directs attention toward different organizational responsibilities. Where technical interpretation is concentrated in one actor, other participants may depend on that actor not only for information but also for the categories through which the event becomes governable.

Across the two cases, capability asymmetry therefore refers to a structural separation between authority to act and capacity to observe, interpret, or verify the relevant technical facts. The resulting operational weakness lies in dependence: an actor may formally possess responsibility for intervention while relying on another organization for information necessary to determine what intervention is warranted.

4.4. Incentive Divergence and Selective Collaboration

The fourth mechanism concerns the continuity of cooperation across organizations whose objectives and costs are not identical. Public authorities, platforms, financial institutions, communications operators, and users may all benefit from reducing deepfake-related harm, but they do not bear the same costs of prevention, information exchange, technical modification, false positives, or service interruption.

The cases indicate that the value of cooperation differs across stages of the governance episode. Once a harmful incident becomes visible, the benefits of reporting, investigation, evidence preservation, and public warning are comparatively clear. Preventive cooperation is more demanding because it requires organizations to invest before the benefits of that investment can be attributed to a specific avoided incident. Routine information exchange, common classifications, technical hardening, and joint review therefore create costs that are immediate even when the benefits remain diffuse.

This distinction helps explain why visible cooperation should not be treated as equivalent to sustained governance capacity. A joint warning, reporting channel, investigation, or post-incident response demonstrates participation, but it does not necessarily establish that information will move in the same way before the next incident

or that previous experience will change later organizational practice. The relevant issue is therefore not whether actors cooperate at all, but when they cooperate, what information they exchange, and whether the cooperation persists beyond a specific incident.

Organizational performance measures can reinforce this difference. Activities such as cases solved, accounts suspended, warnings issued, or items removed are relatively visible, whereas improvements in verification speed, evidence usability, successful handoffs, prevention of repeat incidents, or correction of false positives are harder to observe and attribute. Where measurable outputs dominate evaluation, participation may become visible without demonstrating that the underlying coordination problem has changed [27].

The comparative evidence therefore supports a distinction between formal collaboration and capacity-producing collaboration. Formal collaboration establishes channels, agreements, campaigns, or episodes of joint action. Capacity-producing collaboration changes the operational sequence: relevant information reaches an actor capable of intervention, that information remains interpretable across organizational boundaries, action occurs within the relevant time window, and the outcome can inform subsequent practice. The distinction is one of organizational effect rather than organizational presence (As shown in Table 4).

Table 4. Comparative Summary of the Four Governance Failure Mechanisms

Mechanism	Huangshi voice fraud	Cangnan face changing theft	Common governance implication
Temporal mismatch	Real time persuasion moves faster than verification and technical confirmation	Synthetic identity signals can move through several controls before institutional updating	Rules need operational learning and time sensitive safeguards
Jurisdictional fragmentation	Victim, police, communication, family, and payment actors see different segments	Data, identity, platform, finance, and offline actors own different links	A lead coordination function must own the handoff across the chain
Capability asymmetry	Technical proof and digital traces are controlled outside the victim and frontline unit	Platforms or financial institutions define authentication evidence and control relevant logs	Participation must be accompanied by auditability and independent verification
Incentive divergence	Prevention depends on routine verification and rapid sharing with diffuse benefits	Proactive hardening and data exchange impose costs before harm is visible	Metrics and duties must reward prevention, learning, and fair correction

Taken together, the four mechanisms show that the central divide is not between the presence and absence of governance. It lies between formal governance resources and their conversion into operational capacity. Temporal mismatch affects whether action occurs in time; jurisdictional fragmentation affects whether information survives organizational handoffs; capability asymmetry affects whether relevant facts can be independently established; and incentive divergence affects whether coordination persists beyond individual incidents. The following section examines what these findings imply for asymmetric adaptive coordination as an organizational capability.

5. Discussion

5.1. From Environmental Turbulence to Asymmetric Dependence

The findings refine environmental explanations of deepfake governance by showing that technological turbulence does not produce operational weakness by itself. Rapid

changes in synthetic-media tools increase uncertainty and shorten the time available for institutional response, but their governance effects depend on how information, authority, expertise, and intervention capacity are distributed across organizations. Public authorities may possess legal authority without equivalent technical visibility; platforms may possess detailed operational information without responsibility for the entire harm chain; financial and communications actors may control critical points of intervention; and victims may possess contextual knowledge while lacking the means to verify what occurred. The governance environment is therefore not merely turbulent and interdependent, but structurally asymmetric.

This distinction shifts attention from the speed of technological change to the distribution of adaptive capacity. The same technological risk can generate different governance outcomes depending on who first observes it, who can interpret it, who is authorized to intervene, and whether those capacities can be connected within the relevant time window. Technological turbulence becomes institutionally consequential when the organizations required to adapt depend on resources controlled elsewhere.

The findings therefore extend the conventional idea of institutional lag. Lag is not simply a temporal distance between technological innovation and formal rulemaking. It can persist even after regulation exists because formal authority, factual visibility, technical expertise, and operational intervention remain organizationally separated [28]. The resulting problem is one of asymmetric dependence: governance capacity depends not only on whether institutions adapt, but on whether differently situated actors can combine their capacities without losing time, context, or accountability.

5.2. From Collaboration to Operational Capacity

The findings also clarify why collaboration should not be treated as equivalent to governance capacity. Multi-actor participation becomes operationally consequential only when it produces three transformations. First, dispersed observations must become a shared problem representation. A suspicious voice, an authentication anomaly, a fraud report, and a privacy incident may each describe part of the same episode while directing attention toward different organizational routines. Coordination requires these local descriptions to become mutually intelligible without erasing the distinct responsibilities attached to them. Second, information must become an operational handoff. Information sharing has governance value only when relevant signals reach an actor capable of intervention, remain interpretable across organizational boundaries, and arrive while action is still possible. The existence of reporting channels or cooperation agreements therefore provides only a formal infrastructure. Operational capacity depends on what passes through those channels, when it moves, and whether the receiving organization can act upon it. Third, action must become institutional learning. A governance system may successfully investigate or prosecute an individual incident while remaining vulnerable to repetition if the case does not alter subsequent risk classifications, evidence procedures, technical controls, organizational routines, or public guidance. Response and adaptation are therefore analytically distinct: institutions can respond without learning.

This distinction also qualifies the role of trust in collaborative governance. Trust can reduce transaction costs and support cooperation under uncertainty, but it cannot substitute for verification where information and capability are distributed asymmetrically. At the same time, purely adversarial oversight may discourage early disclosure and joint problem solving. Formal obligations, repeated interaction, and independent review therefore perform different but complementary functions [29, 30]. The central issue is not whether cooperation is formal or informal, but whether it converts dependence into timely, verifiable, and revisable action.

5.3. Adaptive Coordination as an Organizational Capability

The preceding analysis allows asymmetric adaptive coordination to be specified more precisely. It is not simply another form of collaboration, nor does it require eliminating asymmetries among participating actors. Its function is to make those asymmetries governable by connecting capacities that remain institutionally distributed.

Five interrelated capabilities are central to this process. Sensing capacity identifies emerging tools, attack patterns, victim experiences, and recurring anomalies before they are reduced to isolated incidents. Translation capacity allows technical, legal, policing, financial, and public-facing actors to interpret the same event across professional and institutional vocabularies. Orchestration capacity assigns responsibility for interorganizational handoffs and establishes procedures and time expectations for situations in which delayed exchange reduces the possibility of intervention. Learning capacity connects case outcomes to subsequent changes in training, risk categories, evidence standards, platform controls, and regulatory practice. Correction capacity makes intervention revisable through explanation, review, appeal, and remediation when preventive or enforcement measures are excessive or erroneous.

These capacities are analytically distinct but operationally interdependent. Sensing without translation produces signals that cannot travel; translation without orchestration produces shared understanding without coordinated action; orchestration without learning produces repeated case-by-case response; and adaptation without correction risks converting greater intervention capacity into unaccountable power. Asymmetric adaptive coordination therefore concerns the organization of the entire governance cycle rather than the addition of any single institutional instrument.

This perspective has practical implications. Risk-based regulation must be connected to operational thresholds and review cycles rather than remaining at the level of general obligations. Lawful information exchange requires purpose limitation, data minimization, traceable requests, preservation procedures, and accountability. Interorganizational exercises should test the sequence from initial signal to intervention rather than merely confirm the existence of cooperation agreements. Evaluation should similarly extend beyond counts of removals, warnings, or completed cases to indicators such as verification time, handoff quality, evidence usability, victim relief, repeat-incident learning, and correction of erroneous interventions.

The same logic extends to cross-platform and cross-border settings. Distributed authority does not require a single organization to control the entire chain, but it does require the network to remain legible to those operating within it. Actors need to know who is responsible for escalation, what information can lawfully be exchanged, what form that information must take, what response is expected, and how the outcome will be reviewed. Transgovernmental enforcement networks, standardized preservation procedures, platform contact mechanisms, and trusted escalation channels can support such coordination without eliminating institutional boundaries [14].

5.4. Public Values and Proportionality as Boundary Conditions

Greater coordination is not inherently better governance. Measures that improve the speed or integration of intervention can also increase surveillance, biometric-data collection, false positives, restrictions on legitimate synthetic expression, or unreviewable automated decisions. Public values therefore constitute boundary conditions of asymmetric adaptive coordination rather than external considerations added after operational capacity has been established.

This point is particularly important because several capacities identified above can generate competing effects. Faster information exchange can strengthen fraud prevention while expanding access to sensitive personal data. Stronger authentication can reduce impersonation while imposing burdens on legitimate users. Automated detection and blocking can operate at scale while producing opaque or uneven errors [11]. Effective coordination must therefore be evaluated not only by whether it increases intervention capacity, but also by whether that capacity remains proportionate, explainable, and correctable.

Proportionality requires differentiation among forms of risk and response. Labeling, additional verification, temporary restriction, removal, evidence preservation, and referral to law enforcement impose different burdens and should correspond to different levels of expected harm. Identity impersonation linked to financial fraud may justify

stronger and faster intervention than authorized artistic transformation or clearly disclosed satire. Correction mechanisms are equally important because the legitimacy of adaptive governance depends partly on its capacity to revise mistaken decisions rather than merely act quickly.

Public value also requires attention to unequal vulnerability. Individuals differ in their ability to recognize synthetic signals, verify identities, preserve evidence, navigate platform reporting procedures, and obtain institutional assistance. Older victims in voice-fraud contexts, for example, may face different verification burdens from users with greater technical familiarity. Individuals whose images or voices are appropriated may possess contextual knowledge of the harm while lacking access to the technical and organizational resources required to establish it. A governance model that responds to capability asymmetry among institutions while shifting the remaining burden onto individuals would reproduce the very asymmetry it seeks to manage.

Public education, accessible reporting, human review, victim assistance, explanation, and appeal are therefore part of governance capacity rather than peripheral protections. Asymmetric adaptive coordination is effective only when its capacity to sense and intervene is matched by an equivalent capacity to justify, review, and correct its own actions.

6. Conclusion

This article examined why formally developed deepfake-governance arrangements may remain operationally weak even when regulation exists and multiple public and private actors participate. The comparison of the Huangshi AI voice-impersonation fraud case and the Cangnan AI face-swapping theft case identifies four mechanisms underlying this gap: temporal mismatch between technological change and institutional response, jurisdictional fragmentation across the harm chain, regulatory dependence and capability asymmetry, and incentive divergence that makes cooperation selective or episodic.

The findings show that the central problem is not simply the absence of rules or responsible actors, but the failure to convert distributed governance resources into operational capacity. This article conceptualizes that problem as asymmetric adaptive coordination: the capacity to connect changing risks, distributed authority, unequal information and expertise, and divergent incentives through processes of sensing, translation, orchestration, learning, and correction. Effective coordination does not require eliminating these asymmetries, but making them governable while preserving public values such as security, privacy, due process, expression, and public trust.

The study offers a mechanism-based rather than statistically generalizable explanation. Its broader implication is that a governance system can be formally dense and operationally thin. The challenge of deepfake governance is therefore not merely to add rules or participants, but to ensure that institutional presence becomes durable capacity to act, learn, and correct.

References

1. R. Chesney and D. K. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," *California Law Review*, vol. 107, pp. 1753–1819, 2019, doi: 10.2139/ssrn.3213954.
2. J. Kietzmann, L. W. Lee, I. P. McCarthy, and T. C. Kietzmann, "Deepfakes: Trick or treat?," *Business Horizons*, vol. 63, no. 2, pp. 135–146, 2020, doi: 10.1016/j.bushor.2019.11.006.
3. R. Rini, "Deepfakes and the epistemic backstop," *Philosophers' Imprint*, vol. 20, no. 24, pp. 1–16, 2020.
4. C. Vaccari and A. Chadwick, "Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news," *Social Media + Society*, vol. 6, no. 1, pp. 1–13, 2020, doi: 10.1177/2056305120903408.
5. Cyberspace Administration of China, "Provisions on the Administration of Deep Synthesis of Internet-Based Information Services", 2022. [Online]. Available: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm
6. Cyberspace Administration of China, "Interim Measures for the Management of Generative Artificial Intelligence Services", 2023. [Online]. Available: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
7. Cyberspace Administration of China, *Measures on the Identification of AI-Generated Synthetic Content*, 2025. [Online]. Available: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm

8. A. Firc, K. Malinka, and P. Hanáček, "Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors," *Heliyon*, vol. 9, no. 4, p. e15090, 2023, doi: 10.1016/j.heliyon.2023.e15090.
9. M. Westerlund, "The emergence of deepfake technology: A review," *Technology Innovation Management Review*, vol. 9, no. 11, pp. 39–52, 2019, doi: 10.22215/timreview/1282.
10. T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press, 2018.
11. R. Gorwa, R. Binns, and C. Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, vol. 7, no. 1, pp. 1–15, 2020, doi: 10.1177/2053951719897945.
12. J. P. Quintais, N. Appelman, and R. Ó Fathaigh, "Using terms and conditions to apply fundamental rights to content moderation," *German Law Journal*, vol. 24, no. 5, pp. 881–911, 2023, doi: 10.1017/glj.2023.53.
13. R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, vol. 29, no. 3, pp. 408–433, 2006, doi: 10.1108/13639510610684674.
14. T. Legrand and C. Leuprecht, "Securing cross-border collaboration: Transgovernmental enforcement networks, organized crime and illicit international political economy," *Policy and Society*, vol. 40, no. 4, pp. 565–586, 2021, doi: 10.1080/14494035.2021.1975216.
15. J. D. Thompson, M. N. Zald, and W. R. Scott, *Organizations in Action: Social Science Bases of Administrative Theory*. London, U.K.: Routledge, 2017.
16. T. Burns and G. M. Stalker, *The Management of Innovation*, 3rd ed. Oxford, U.K.: Oxford University Press, 1994.
17. S. Park, D. S. Lee, and J. Son, "Regulatory reform in the era of new technological development: The role of organizational factors in the public sector," *Regulation & Governance*, vol. 15, no. 3, pp. 894–908, 2021, doi: 10.1111/rego.12339.
18. H. W. J. Rittel and M. M. Webber, "Dilemmas in a general theory of planning," *Policy Sciences*, vol. 4, no. 2, pp. 155–169, 1973, doi: 10.1007/BF01405730.
19. R. Agranoff, *Managing within Networks: Adding Value to Public Organizations*. Washington, DC: Georgetown University Press, 2007.
20. H. Wang and B. Ran, "Network governance and collaborative governance: A thematic analysis on their similarities, differences, and entanglements," *Public Management Review*, vol. 25, no. 6, pp. 1187–1211, 2023, doi: 10.1080/14719037.2021.2011389.
21. C. Ansell and A. Gash, "Collaborative governance in theory and practice," *Journal of Public Administration Research and Theory*, vol. 18, no. 4, pp. 543–571, 2008, doi: 10.1093/jopart/mum032.
22. L. Poppo and T. Zenger, "Do formal contracts and relational governance function as substitutes or complements?," *Strategic Management Journal*, vol. 23, no. 8, pp. 707–725, 2002, doi: 10.1002/smj.249.
23. P. S. Ring and A. H. Van de Ven, "Developmental processes of cooperative interorganizational relationships," *Academy of Management Review*, vol. 19, no. 1, pp. 90–118, 1994, doi: 10.2307/258836.
24. A. L. George and A. Bennett, *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.
25. D. Collier, "Understanding process tracing," *PS: Political Science & Politics*, vol. 44, no. 4, pp. 823–830, 2011, doi: 10.1017/S1049096511001429.
26. J. Gerring, *Case Study Research: Principles and Practices*. Cambridge, U.K.: Cambridge University Press, 2007.
27. S. L. Benaine, "Performance gaming: A systematic review of the literature in public administration and other disciplines with directions for future research," *International Journal of Public Sector Management*, vol. 33, no. 5, pp. 497–517, 2020, doi: 10.1108/IJPSM-07-2019-0191.
28. A. Taeihagh, "Governance of generative AI," *Policy and Society*, vol. 44, no. 1, pp. 1–22, 2025, doi: 10.1093/polsoc/puaf001.
29. A. C. Inkpen and S. C. Currall, "The coevolution of trust, control, and learning in joint ventures," *Organization Science*, vol. 15, no. 5, pp. 586–599, 2004, doi: 10.1287/orsc.1040.0079.
30. S. S. Lui and H.-Y. Ngo, "The role of trust and contractual safeguards on cooperation in non-equity alliances," *Journal of Management*, vol. 30, no. 4, pp. 471–485, 2004, doi: 10.1016/j.jm.2004.02.002.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of Publisher and/or the editor(s). Publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.