Social Science Chronicle

OPEN ACCESS

Peer-Reviewed, International, Academic Research Journal

ISSN : 3048-6297

RESEARCH ARTICLE

Artificial Intelligence and Big Data in Global Politics: How AI and ML Influence Power, Governance, Democracy, International Relations, Misinformation and Polarization?

Félix Carrillo[1]*

[1] Universidade Federal de Sergip, Sergipe, Brazil.

** Corresponding Author*
E-mail : carrillofelix@rediffmail.com

Citation
Carrillo, F. (2026). Artificial Intelligence and Big Data in Global Politics: How AI and ML Influence Power, Governance, Democracy, International Relations, Misinformation and Polarization?. *Social Science Chronicle*, Vol. 6, pp. 1-11.

Digital Object Identifier (DOI)
https://doi.org/10.56106/ssc.2026.004

Received - October 19, 2025
Accepted - February 5, 2026
Published - April 24, 2026

Web-Link
All contents of this peer-reviewed article, along with other relevant details are available at:
http://socialsciencechronicle.com/article-ssc-2026-004

Copyright
The copyright of this article is reserved with the author/s.
© 2026, Félix Carrillo.

This publication is distributed under the terms of Creative Commons Attribution, Non-Commercial, Share Alike 4.0 International License. It permits unrestricted copying and redistribution of this publication in any medium or format.

Abstract

This article theorizes artificial intelligence as a power-bearing political infrastructure that reconfigures authority, legitimacy, representation, and strategic order across contemporary polities. Rather than treating AI as a neutral efficiency technology, the article frames it as an institutionalized regime of probabilistic inference, classification, and attention allocation that redistributes *infrastructural power* toward actors with asymmetric access to data, compute, expertise, and distribution channels. It develops a political science analytic architecture that integrates *three-dimensional power*, *non-domination*, *principal-agent* delegation, *historical institutionalism* pathways of layering and drift, and political behavior constructs such as *bounded rationality*, *motivated cognition*, and *affective polarization*. Within democratic arenas, AI-mediated micro-segmentation and ranking logics are analyzed as mechanisms of agenda control and information discrimination that weaken shared publicity, dilute accountability, and shift influence from contestable persuasion toward manipulative optimization. Within the administrative state, algorithmic governance is treated as a transformation of discretion, where authority migrates upstream into objective-setting, proxy construction, threshold calibration, and lifecycle updating, generating contestability deficits, administrative burdens, and accountability gaps intensified by procurement lock-in and proprietary enclosure. At the international level, the article conceptualizes AI as strategic infrastructure embedded in supply-chain dependencies and regime complexity, producing security dilemma dynamics, epistemic fragility in crisis decision cycles, and scalable information operations that target cognitive security and institutional trust. The synthesis yields a compact typology of political effects and governance risks, and articulates institutional design principles for democratic steering that prioritize procedural intelligibility, auditability, enforceable remedy pathways, and rights-consistent constraints on surveillance and targeting. The article offers a cross-sector, globally oriented conceptual toolkit for academics, policymakers, industry actors, and students navigating algorithmic polities under conditions of accelerated, transnational, datafied power.

Keywords
Artificial Intelligence, Algorithmic Governance, Political Communication, Computational Propaganda, Disinformation, Electoral Integrity, Micro-targeting, Political Polarization, Surveillance, Digital Authoritarianism, Democratic Backsliding, Platform Governance, Data Privacy, International Security.

1. Introduction

Artificial intelligence is now a general-purpose capability that re-organizes political life by accelerating inference, automating classification, and industrializing persuasion across digital infrastructures. The central problem is not whether AI enters politics, but how it reshapes the distribution of power, the architecture of legitimacy, and the feasibility of democratic control under conditions of scale, opacity, and rapid adaptation (Subekti et al., 2025; Alcoforado et al., 2024; Momeni, 2025). This article treats AI as both an instrument deployed within political competition and an infrastructural substrate that conditions what is visible, actionable, and governable in contemporary polities. The scope is deliberately conceptual-theoretical, focusing on mechanisms that connect AI to electoral competition, party organization, public administration, legal accountability, platform rulemaking, and geopolitical rivalry. The guiding premise is that AI changes political equilibria by altering transaction costs, information asymmetries, and coordination possibilities, thereby reconfiguring representation, state capacity, and contestability in ways that demand institutional design responses rather than purely technical remedies.

Conceptual Boundaries and Operational Definitions for Political Analysis

For political analysis, AI is defined as a class of computational systems that produce probabilistic judgments and generative outputs by learning from data, enabling prediction, ranking, recommendation, identification, and content synthesis. This includes recommender systems, predictive analytics, biometric recognition, risk scoring, decision-support automation, and generative models that compress production costs for text, image, audio, and video (Walker et al., 2024; Yigitcanlar et al., 2024). Politics is defined as structured contestation over authority, resources, meaning, and coercion under formal rules and informal norms, encompassing electoral competition, governance, jurisprudence, and the management of collective life. Three influence modalities are analytically separated. Persuasion is influence compatible with agency and public contestation. Manipulation exploits cognitive vulnerabilities or informational asymmetries while reducing transparency and reciprocity. Coercion is influence grounded in credible sanctioning power. These boundary conditions prevent category collapse, keeping normative assessment anchored in institutional standards, procedural justice, and rights-based constraints rather than in technocratic performance metrics alone.

Why Political Science is Necessary for AI-Political Diagnostics?

Technical descriptions of AI commonly focus on accuracy, efficiency, and model behavior, yet political consequences arise from how AI redistributes authority, restructures accountability chains, and recalibrates legitimacy under contested values. Political science supplies the diagnostic grammar for these shifts by foregrounding power, institutions, collective action, delegation, political behavior, and political economy. A principal-agent lens clarifies how responsibility diffuses across voters, executives, agencies, vendors, and models, enabling blame displacement and institutional ambiguity. Institutionalism explains why AI adoption often proceeds through layering, drift, and conversion, producing path dependence and lock-in. Political behavior frameworks clarify how identity, heuristics, motivated cognition, and affective polarization interact with personalization and attention engineering. Political economy adds distributional clarity by locating rents, monopoly power, and asymmetric exposure to surveillance and error costs. International relations theory extends the analysis to strategic competition, information operations, and regime complexity, where verification problems and escalation risks make governance a security and diplomacy problem, not merely a compliance problem.

Guiding Analytic Architecture for Theoretical Synthesis

The article is organized around a stable analytic architecture that travels across all sections, enabling cumulative reasoning without repetition. First are actors whose strategic preferences are shaped by incentives and constraints, including parties, executives, agencies, courts, platforms, vendors, civil society, and security institutions. Second are institutions that allocate authority and structure contestation, including electoral rules, administrative law, constitutional constraints, federal arrangements, and informal norms of legitimacy. Third are resources that condition political advantage, including data access, compute capacity, expertise, legal authority, financial capital, and attention as a scarcity-managed commodity. Fourth are mechanisms that translate AI into political effects, including agenda control through ranking, persuasion through microsegmentation, surveillance through identity resolution, delegation through procurement, and automation through standardized classification. Finally are feedback loops, where AI-enabled governance produces constituencies, sunk-cost dependence, and adaptive counter-moves, generating dynamic equilibria rather than stable end states. This architecture supports a theory-first narrative that stays sensitive to heterogeneity across regime types, administrative capacity, and geopolitical position.

Normative Evaluation Criteria for Multisector Readerships

The article evaluates AI in political life using criteria that are actionable for policy makers, interpretable for students, and operationally meaningful for industry and governance professionals. Democratic political equality requires that influence, information access, and administrative error costs are not systematically skewed by segmentation, proxy classification, or uneven contestability. Legitimacy is treated as a composite of input responsiveness, throughput

procedural integrity, and output performance, with special attention to contestation rights, intelligibility of reasons, and effective remedy pathways. Non-domination frames AI as a risk of arbitrary power when surveillance and automated decisions become difficult to contest, even if formally lawful. The article proceeds from foundations to consequences and governance by moving through political science core concepts, infrastructural power shifts, democratic institutions and the algorithmic public sphere, state bureaucracy and law, and the international order. This trajectory is designed to deliver decision-relevant frameworks, governance design principles, and conceptual tools that can be translated into procurement standards, oversight mandates, institutional safeguards, and civic resilience strategies without relying on empirical case narration.

2. Political Science Foundations for Analyzing AI

Power, Domination, and Agenda Control in Computational Polities

A political science diagnosis of AI begins with power as relational capacity to shape outcomes, constrain options, and structure the field of contestation. AI intensifies decision power by compressing uncertainty through prediction, it amplifies agenda power by ranking visibility and allocating attention, and it extends preference-shaping power by tailoring persuasive cues to identity and affect (Jacobs, 2024; Foos, 2024). This triadic structure aligns with three-dimensional power because the most consequential effects often occur upstream of explicit choice, within salience engineering, default design, and classification regimes that pre-sort populations into administratively meaningful categories such as risk, eligibility, credibility, and threat. AI also operationalizes domination when individuals face arbitrary interference without reliable routes of explanation, contestation, and remedy, turning probabilistic inference into de facto authority. Political control becomes infrastructural, embedded in platforms, data pipelines, and model objectives that quietly govern what is thinkable, shareable, and actionable across the polity.

Legitimacy, Authority, and Political Obligation Under Automated Rule Systems

Legitimacy in AI-mediated governance is best treated as a composite of input legitimacy, throughput legitimacy, and output legitimacy, each vulnerable to distinct algorithmic pathologies. Input legitimacy degrades when segmented information environments fracture common agendas and undermine shared accountability, producing selective responsiveness optimized for mobilization rather than representation (Mahony & Chen, 2025; Michels, 2024). Throughput legitimacy weakens when decisions become procedurally thin, epistemically opaque, and practically non-contestable, creating a contestability deficit even where formal legality remains intact. Output legitimacy becomes fragile when error costs, delays, and denials concentrate on structurally disadvantaged groups, converting statistical artifacts into lived inequality. Authority under automation can also acquire a false aura of neutrality through automation bias and the objectivity illusion, which misrecognize value-laden choices in data selection, proxy construction, and optimization as purely technical necessities. Political obligation cannot be sustained by performance alone, it requires intelligible reasons, procedural reciprocity, and institutionalized avenues for challenge that transform algorithmic outputs into governable, revisable public decisions.

Institutionalism, Delegation, and Accountability Architectures in Algorithmic States

Institutional analysis treats AI adoption as a mode of incremental transformation rather than a discrete technological substitution, operating through layering, drift, and conversion that rewire authority while preserving familiar administrative forms. Layering occurs when decision-support tools become informal decision rules, drift emerges when legal categories lag behind technical practices, and conversion appears when agencies repurpose existing mandates to govern AI without explicit authorization (Ge, 2024; Charalabidis et al., 2024). These pathways produce path dependence and lock-in through sunk costs, vendor dependence, and routinized metrics that become politically costly to abandon. Delegation theory clarifies how accountability attenuates across nested principal-agent chains, voters delegate to officials, officials to agencies, agencies to vendors, and vendors to models whose objectives and thresholds encode consequential value judgments. Agency loss concentrates in design moments that rarely appear in public oversight, such as proxy selection, threshold setting, retraining cadence, and incident handling. Robust accountability architecture therefore requires traceable responsibility, auditable decision records, and procedural constraints that prevent discretion from disappearing into technical black boxes.

Collective Action, Political Behavior, and Persuasion Under Algorithmic Mediation

AI intensifies classic collective action problems because information integrity, privacy, and election legitimacy function as public goods that are underprovided when competitive incentives reward defection. Parties, platforms, and intermediaries face escalation dynamics, adopting ever more granular targeting and content optimization because rivals can do so, even when system-level harms increase (Haesevoets et al., 2024; Ahmed et al., 2025). Political behavior theory explains why these harms scale, citizens operate under bounded rationality, rely on heuristics, and exhibit motivated reasoning that filters evidence through identity commitments and affect. Recommender architectures can exacerbate affective polarization by prioritizing high-arousal content, reinforcing identity sorting, and converting political communication into continuous attention competition. Influence pathways can be analytically separated into persuasion compatible with autonomy, manipulation that exploits cognitive vulnerabilities or informational asymmetries, and coercion grounded in sanctioning capacity, with AI shifting the margin toward manipulation by lowering production costs,

accelerating iteration, and reducing public visibility of claims. Democratic resilience therefore depends on institutional designs that restore shared publicity, dampen exploitative targeting, and strengthen contestability in both electoral and administrative domains.

Political Economy and International Order of AI as Strategic Infrastructure

The political economy of AI foregrounds distribution, rents, and structural dependency, data access, compute capacity, and proprietary standards become strategic assets that concentrate advantage and create barriers to democratic steering. Platform governance and vendor ecosystems can function as private rulemaking apparatuses, generating quasi-constitutional effects on speech, association, and political advertising while remaining weakly accountable to public authorization (Nwosu et al., 2024; Radanliev, 2025). Regulatory capacity is shaped by capture risks, procurement lock-in, and asymmetries of expertise, which can shift policy from rights-based governance toward market-convenient compliance theater. At the international level, AI introduces security dilemma dynamics because states interpret rivals' capabilities under uncertainty, leading to competitive accumulation of data, compute, and influence tools that can escalate mistrust. Global governance exhibits regime complexity, overlapping forums, fragmented standards, and verification difficulties that impede enforceable commitments, especially when AI is securitized as critical infrastructure. The result is a coupled system in which domestic legitimacy and international stability are jointly conditioned by the governance of transnational infrastructures, supply chains, and information operations, making institutional design a geopolitical as well as democratic imperative.

3. AI as Political Infrastructure and Re-configuration of Power

Tools and Political Infrastructures

Artificial intelligence functions politically less as a discrete instrument and more as an infrastructural layer that standardizes perception, allocates visibility, and routinizes decision cycles across digital and administrative systems. Infrastructure has distinctive political properties, it is backgrounded, it becomes difficult to exit, and it creates path dependence through sunk costs, interoperability constraints, and institutional habituation (Romanishyn et al., 2025; Hunter et al., 2024). When AI is embedded in identity verification, content ranking, service eligibility, and security triage, it quietly rewrites the default conditions of governability by lowering the marginal cost of monitoring, accelerating feedback loops, and compressing administrative time. This shifts advantage toward actors with persistent access to data, compute, and organizational expertise, creating infrastructural power that outlives electoral turnover and resists episodic oversight. The operational locus of power moves upstream into objective-setting, metric selection, and pipeline governance, making control over standards, interfaces, and auditability as politically consequential as control over formal rules.

Politics of Classification and Proxy Governance

Modern political order depends on classification, who is eligible, risky, credible, compliant, or suspect, and AI intensifies classification by translating messy social life into machine-legible categories via proxies. Proxy governance arises when latent attributes are inferred from behavioral traces, geolocation patterns, social graphs, and linguistic markers, then used to allocate opportunities, burdens, or scrutiny. This produces a political problem of categorical authority, because classification decisions embed normative judgments about deservingness, threat, and priority while presenting outputs as neutral inference (Haq et al., 2024; Ahmad et al., 2025). In practice, the most consequential choices occur in feature construction, label definition, threshold calibration, and error-cost allocation, each of which distributes harm and benefit asymmetrically. The political risk is not only misclassification, but also category lock-in, where administratively convenient proxies harden into quasi-legal identities that are difficult to contest. A concrete diagnostic is to map every classification to its proxy variables, decision thresholds, appeal pathways, and differential burden across groups.

Opacity, Expertise, and Technocratic Authority

AI expands the domain of epistemic asymmetry by creating decision systems whose rationales are difficult to render into public-reasonable explanations, even when outputs can be measured. Opacity is not merely technical complexity, it is also organizational secrecy, proprietary enclosure, and procedural minimalism that together weaken contestability. This environment elevates expertise into a gatekeeping resource, enabling technocratic authority in which model performance becomes a substitute for democratic justification, and compliance artifacts become a substitute for accountability (Best et al., 2024; Sieber et al., 2025). The authority shift is reinforced by automation bias and institutional risk-aversion, where decision-makers defer to model outputs to avoid blame, converting probabilistic scores into de facto commands. A rigorous theoretical response treats explainability as legal intelligibility and actionable contestation, not as interpretability theater. Concretely, governance must require traceable decision logs, documented objective functions, disclosed proxy families, and enforced rights to challenge both outcomes and the classification logic that produced them.

Attention Architectures and Manufactured Salience

Political conflict is mediated through attention, and AI-driven ranking systems operate as salience machines that reconfigure agenda setting, framing, and priming at planetary scale. By optimizing for engagement, retention, or interaction velocity, recommender systems can privilege high-arousal content, accelerate moralized narratives, and stratify publics into micro-audiences with divergent

informational baselines. This produces manufactured salience where what appears socially important is partly an artifact of optimization targets, interface defaults, and amplification dynamics rather than deliberative priority (Mead, 2024; Łabuz & Nehring, 2024). The resulting polity is characterized by fragmented publicity, variable issue agendas, and differential exposure to persuasive stimuli, which undermines common accountability and enables selective responsiveness. The actionable analytic move is to treat ranking objectives as political choices, identify the optimization metrics, friction settings, and amplification thresholds, and evaluate how each setting affects visibility distribution, cross-cutting exposure, and the feasibility of shared public reasoning. Institutional safeguards must focus on publicity conditions, not only on content truth-values.

Behavioral Governance, Surveillance, and Feedback Lock-in

AI enables behavioral governance by coupling microsegmented persuasion with continuous monitoring, turning influence into an adaptive control problem that iterates on what moves attention, emotion, and action. Personalized messaging can shift the influence frontier from persuasion toward manipulation when it exploits informational asymmetries, leverages identity cues, and reduces the possibility of public contestation through audience fragmentation. Surveillance intensifies this dynamic by providing dense feedback signals, location traces, biometric identifiers, and network embeddings that allow actors to model susceptibility and intervene with precision, producing chilling effects on association and dissent even without overt coercion (Margetts & Dunleavy, 2024; Sienknecht & Vetterlein, 2024). Over time, deployment generates policy feedback and lock-in, agencies, vendors, and political coalitions become invested in the system's continuation, while withdrawal is framed as operational risk. The concrete control points are targeting constraints, disclosure rules, limits on sensitive-attribute inference, mandatory appeal routes, and lifecycle oversight that detects drift, feedback amplification, and Goodhart effects before they become institutionalized as normal governance.

4. Democracy, Elections, Parties and Algorithmic Public Sphere

Representation and Party Competition in Fragmented Publics

AI-mediated personalization fractures publicity into segmented issue-spaces, stressing classical representation logics such as the delegate model and trustee model, because the governed no longer encounter a shared agenda against which promises and performance can be collectively evaluated. Under conditions of micro-audience differentiation, spatial competition drifts from common-position signaling toward modular messaging that optimizes distinct coalitional slices, weakening the disciplining force of public scrutiny (Tosi et al., 2025; Scoggins & Robertson, 2024). The representational linkage between preference aggregation and policy responsiveness becomes more contingent on attention allocation, narrative salience, and identity-coded cues, which reshapes issue ownership and valence politics into platform-conditioned contests over visibility. Party strategy can become more metricized and tactical, privileging mobilization efficiency over programmatic coherence, and intensifying cartelization risks when incumbency advantages combine with superior data access. Democratic accountability then requires institutionalized publicity conditions, not merely procedural elections, because representation depends on shared informational baselines and contestable claims.

Campaign Optimization, Data-Driven Parties, and Strategic Escalation

Campaigns become optimization enterprises when AI compresses experimentation cycles, enabling rapid A-B iteration, psychographic inference, and message adaptation within constrained attention budgets. Parties evolve into hybrid organizations that blend ideological branding with computational logistics, shifting internal authority toward analytics teams, vendors, and platform intermediaries who control targeting primitives, attribution models, and conversion metrics (Wadipalapa et al., 2024; Novelli et al., 2024). This reorganizes intra-party governance by privileging what is measurable, scalable, and immediately mobilizing, thereby altering candidate selection, agenda prioritization, and resource allocation. Competitive pressures generate strategic escalation where actors adopt increasingly granular targeting because rivals can, even when system-level harms rise, a dynamic consistent with collective-action failure under adversarial incentives. The resulting political market approximates continuous campaigning, with persuasion modeled as micro-level behavior change rather than public reasoning. Governance-relevant control points therefore include disclosure of targeting criteria, constraints on sensitive attribute inference, auditability of vendor pipelines, and procedural commitments that preserve programmatic accountability across micro-segmented electorates.

Micro-targeting, Political Equality, and Information Discrimination

Microtargeting challenges democratic equality by enabling differential persuasion intensities and asymmetric informational environments, producing information discrimination where groups receive divergent claims, framings, and emotional triggers with minimal public visibility. Even when messages are not false, selective omission, context stripping, and affect priming can erode political equality by altering who is nudged, at what frequency, and under which cognitive load conditions (Battista, 2024; Lemke et al., 2024). This shifts the normative baseline from equal formal access to ballots toward equal conditions of influence, which requires attention to exposure, transparency, and contestability. The core theoretical defect is a publicity deficit, claims become non-falsifiable in the public sphere because they are not commonly observable, undermining collective accountability and facilitating opportunistic inconsistency. Institutional remedies must therefore be framed as visibility and contestation infrastructures, including standardized

political communication disclosures, constraints on dark-pattern persuasion, parity rules for message archives, and enforceable rights to know why an individual was targeted, thereby converting opaque influence into contestable political communication.

Synthetic Media, Epistemic Security, and the Crisis of Public Reason

Generative systems reduce the marginal cost of plausible text, voice, and video, amplifying epistemic volatility by accelerating misinformation diffusion and enabling reputational sabotage at scale. The central political harm is not only falsehood, but the destabilization of shared verification norms, which enables the liar's dividend where authentic evidence is dismissed as synthetic, weakening accountability through manufactured doubt (Lahdili et al., 2024; Al Lily, 2025). Public reason depends on stable epistemic institutions, credible signals, and contestable claims, yet algorithmic ranking can privilege virality over veracity, intensifying narrative cascades and emotional contagion. The theoretical problem is a breakdown in epistemic commons, where verification becomes privately costly and publicly underprovided, creating a public-goods failure in informational integrity. Actionable safeguards therefore require provenance mechanisms, rapid correction amplification, institutional crisis-communication protocols, and procedural commitments that prioritize contestability over takedown theater. A governance stance grounded in procedural legitimacy emphasizes audit trails, transparent moderation rationales, and remedies for affected speakers and audiences, preserving free expression while stabilizing epistemic security.

Platform Constitutionalism, Electoral Management Legitimacy, and Civic Resilience

Platforms increasingly operate as quasi-constitutional rulemakers that govern speech visibility, association patterns, and political advertising infrastructures, yet their authority often lacks democratic authorization and robust due process, producing legitimacy deficits in platform constitutionalism. Electoral management bodies face parallel challenges when AI-supported roll maintenance, fraud triage, or resource allocation is perceived as opaque or partisan, because perceived fairness is as politically consequential as technical performance (Nie, 2024; Erskine, 2024). Legitimacy in these domains requires contestability, intelligible reasons, and effective remedies, not merely compliance artifacts, because governance that cannot be challenged becomes experienced as arbitrary power. Civic resilience is therefore an institutional capacity, the ability to absorb informational shocks, coordinate trusted communication, and maintain procedural confidence under adversarial manipulation. Concrete resilience levers include independent oversight with enforceable transparency obligations, cross-platform coordination protocols for election periods, standardized appeal pathways for moderation and administrative decisions, and public-interest access to audit-relevant data under privacy-preserving constraints. The objective is to restore shared publicity, reduce arbitrary interference, and sustain democratic steering in a high-velocity algorithmic environment.

5. State, Bureaucracy, Law and Algorithmic Governance

Street-Level Bureaucracy and Discretion Under Model-Driven Administration

AI does not eliminate administrative discretion, it relocates it across the decision chain, transforming street-level bureaucracy into a distributed regime of design-time and run-time judgments. Discretion migrates from frontline caseworkers toward model developers, policy analysts, procurement officers, and managers who set objectives, thresholds, and escalation rules, thereby converting tacit professional judgment into parameterized governance. This reallocation produces discretion by proxy, where eligibility, priority, and risk are operationalized through feature sets and decision rules that can be stable, scalable, and yet normatively loaded. The bureaucratic state becomes a cybernetic control apparatus in which feedback, monitoring, and optimization compress administrative time, intensifying standardization pressures and reducing space for contextualized equity. The governance problem is institutional, how to preserve individualized justice, reason-giving, and accountable discretion when decision authority is partially embedded in socio-technical pipelines that are resilient to episodic supervision.

Administrative Burden, Procedural Friction, and Substantive Citizenship

Algorithmic governance can reconfigure administrative burden by shifting the costs of access, compliance, and appeal onto citizens through opaque denials, documentation inflation, and interaction designs that privilege machine-legibility over human comprehension. Even when nominal rights remain unchanged, burdens can function as covert rationing, producing distributive effects through time costs, cognitive load, and procedural fatigue (Gemenis, 2024; Walter, 2024). The result is a stratified citizenship in which navigational capacity, digital literacy, and legal knowledge determine who converts entitlements into outcomes. This dynamic can be modeled as transaction-cost politics, where AI reduces state processing costs while increasing claimant-side costs, thereby altering welfare-state equilibria without overt policy change. A normatively defensible administrative system must treat friction as a constitutional variable, ensuring that interfaces, forms, and verification routines are not engineered as deterrence mechanisms.

Due Process, Contestability, and Rule-of-Law Constraints on Automation

The rule of law requires that public decisions are knowable, reasoned, and challengeable, yet automated systems can erode these properties by rendering reasons

statistically encoded and operationally inaccessible. Due process in algorithmic administration is not satisfied by abstract transparency narratives, it depends on contestability infrastructures that provide notice, intelligible grounds, meaningful opportunity to respond, and effective remedies (Islam et al., 2024; Kan, 2024). Contestability must extend beyond outcomes to the decision logic, including proxy variables, threshold choices, and update policies that can change eligibility realities without formal rulemaking. Without this, automation can create procedural thinness, where the appearance of neutrality masks arbitrary interference, undermining legitimacy and generating compliance by opacity rather than consent. Institutional safeguards should therefore require decision logging, structured reason statements, appeal pathways with human review capacity, and enforceable limits on automated adverse actions in high-stakes domains. These constraints convert probabilistic inference into publicly governable administrative judgment.

Accountability Architectures, Delegation Chains, and Procurement Political Economy

Accountability in algorithmic states is threatened by nested delegation, voters delegate to officials, officials to agencies, agencies to vendors, and vendors to models whose objectives encode value choices while dispersing responsibility. This creates accountability gaps that enable blame shifting, audit evasion, and symbolic compliance, particularly when proprietary systems limit inspection and when expertise asymmetries constrain oversight (Dunleavy & Margetts, 2025; Zidouemba, 2025). Procurement becomes a political economy site where vendor lock-in, contract opacity, and interoperability constraints harden technical choices into institutional commitments, generating path dependence that is costly to reverse. Robust accountability architecture therefore requires traceable responsibility allocations across the lifecycle, from problem formulation to decommissioning, with auditable documentation of objective functions, data provenance categories, performance monitoring, and incident response. Governance must also anticipate Goodhart effects, where performance metrics become targets and distort behavior, and model drift, where changing environments degrade fairness and validity. The aim is to re-couple delegated authority with enforceable responsibility under public law.

Regulatory Design, Separation of Powers and Public Value Governance

Effective AI governance is an institutional design problem situated within separation-of-powers constraints, where executive capacity, legislative oversight, and judicial review must be recalibrated for adaptive systems. Over-centralization can produce executive aggrandizement through standardized decision pipelines and cross-agency data integration, while under-regulation yields fragmented accountability and regulatory arbitrage across sectors (Wei et al., 2024; Volkivskyi et al., 2024). A coherent approach treats regulation as risk governance with proportional constraints, combining ex ante controls on high-stakes uses with ex post liability, auditability, and remedy mechanisms that preserve democratic steering. The normative benchmark is public value governance, where efficiency is subordinated to legitimacy, equity, and rights-protection, and where transparency is framed as procedural intelligibility and enforceable contestability rather than disclosure theater. Regulatory institutions must also build epistemic capacity, enabling independent evaluation, adversarial testing, and continuous monitoring without collapsing into technocracy. The goal is durable, revisable governance that keeps automated authority within democratically authorized bounds.

6. International Order, Security and Global Political Economy of AI

Sovereignty, Jurisdiction, and the Rewiring of Authority in Datafied Space

AI reconfigures sovereignty by relocating effective control from territorial boundaries toward transnational infrastructures that govern data flows, cloud provisioning, identity resolution, and platform-mediated speech. Sovereignty becomes stratified into legal jurisdiction, technical control, and infrastructural dependency, with each layer vulnerable to asymmetries in compute access, standards ownership, and cross-border interoperability mandates (Cupać et al., 2024; Armiwulan et al., 2024). The resulting condition resembles networked sovereignty, where state authority is exercised through gateways, certification regimes, procurement rules, and data localization strategies that aim to reassert control over informational assets while preserving economic integration. This generates chronic tension between digital constitutionalism and security-driven exceptionalism, because states seek both rights-protective legitimacy and preemptive capacity in surveillance and risk analytics. A coherent theoretical lens treats sovereignty as an evolving bundle of claims over visibility, enforceability, and narrative authority, making institutional design around jurisdictional coordination and contestability a core security variable.

Great-Power Competition, Security Dilemmas, and Escalation Under Algorithmic Uncertainty

AI intensifies strategic competition by compressing decision cycles, amplifying intelligence-processing capacity, and expanding influence operations, while simultaneously increasing uncertainty about adversary capabilities and intent. This produces a classic security dilemma where defensive investments in data, compute, and predictive systems can be interpreted as offensive preparation, elevating threat perceptions and accelerating arms-race dynamics (Marwala, 2024; Stanger et al., 2024). Strategic stability weakens when automated early-warning analytics and anomaly detection are treated as authoritative signals, because false positives and model drift can trigger rapid escalation in crisis environments characterized by bounded attention and political time compression. The problem is not only technical fallibility, it is epistemic fragility within command chains, where automation bias, bureaucratic blame-avoidance, and institutional incentives can privilege

speed over verification. A conceptually rigorous response emphasizes crisis governance design, incorporating redundancy, deliberative friction, and accountable human judgment as stabilizing mechanisms that counteract automation-induced escalation pressures.

Information Operations, Cognitive Security and Industrialization of Persuasion

AI-enabled influence operations operate as continuous, adaptive interventions into attention, affect, and belief formation, transforming persuasion into a scalable optimization problem. The core mechanism is cognitive security degradation, where targeted narrative seeding, synthetic media, and microsegmented messaging erode shared epistemic baselines, amplify distrust, and weaken institutional legitimacy without requiring territorial conquest (Bode, 2024; Baele et al., 2024). This can be modeled as strategic communication under asymmetric visibility, because attackers exploit fragmented publicity and platform ranking to distribute claims that are difficult to collectively observe and contest. Generative systems lower production costs for multilingual content, persona consistency, and rapid iteration, enabling high-volume experimentation that exploits heuristics, identity cues, and moral-emotional triggers. The political risk is epistemic capture, where publics become governable through engineered salience rather than deliberation. Defensive governance therefore requires provenance systems, rapid attribution protocols, cross-platform integrity coordination, and public-interest transparency that preserves free expression while restoring contestability.

Global Governance, Regime Complexity, and Norm Contestation in AI Regulation

Global AI governance is best conceptualized as regime complexity, a fragmented ecology of overlapping institutions, standards bodies, trade rules, security alliances, and human-rights frameworks that generate inconsistent obligations and forum shopping incentives. Binding coordination is difficult because verification is hard, definitions are contested, and states diverge on the legitimacy of surveillance, content control, and strategic autonomy (Kiggins, 2025; Kretsos et al., 2024). Norms emerge through norm entrepreneurship, policy diffusion, and standards competition, with technical specifications functioning as de facto governance instruments that embed values into interoperability constraints and compliance architectures. This produces norm contestation around transparency, accountability, safety, and freedom, where identical vocabulary can mask divergent institutional commitments. A theoretically coherent approach treats global governance as a negotiation over legitimate authority in socio-technical systems, requiring modular instruments that can travel across jurisdictions, baseline procedural guarantees for contestability, and mechanisms for incident reporting and coordinated response that reduce externalities without imposing a single ideological template on heterogeneous polities.

Technology Diplomacy, Supply-Chain Power, and Compute as a Strategic Resource

AI capabilities are conditioned by supply chains, semiconductor ecosystems, cloud concentration, and energy-intensive compute provisioning, making the international political economy of AI a contest over chokepoints, dependencies, and credible access guarantees. Compute functions as a quasi-strategic resource with dual-use implications, enabling both civilian productivity and security applications, which invites securitization and industrial policy measures that reshape markets through export controls, investment screening, and procurement preferences (Wong, 2025; Erman & Furendal, 2024). Technology diplomacy becomes bargaining over standards, certification, and trusted infrastructure, where alliances coordinate to reduce vulnerability while rivals pursue substitution, redundancy, and domestic capacity-building. This resembles geoeconomic statecraft, using market access and supply-chain positioning as tools of influence rather than relying solely on military power. A governance-relevant theoretical stance treats supply-chain resilience, auditability, and interoperability as legitimacy and security issues, because dependency structures determine whether states can enforce rights-based constraints or drift toward exceptional measures under perceived strategic scarcity.

7. Conclusion

This article has treated AI as a power-bearing infrastructure that reorganizes political competition, administrative authority, and global order by compressing uncertainty, scaling classification, and industrializing persuasion. Rather than understanding AI as a discrete tool or neutral efficiency device, it is conceptualized here as a layered socio-technical system embedded in markets, bureaucracies, and security institutions. The core theoretical claim is that the dominant risks are institutional, not merely technical, because AI shifts decision loci upstream into objective-setting, proxy construction, threshold calibration, and lifecycle updating—sites where democratic contestation is typically weakest and least visible. What appears downstream as automated output is often the product of upstream political choices that escape ordinary scrutiny. Across regimes, AI amplifies infrastructural power by privileging actors with persistent access to data, compute, expertise, and distribution channels, while simultaneously eroding throughput legitimacy through opacity, contestability deficits, and responsibility diffusion. The democratic stress test is therefore procedural and relational: whether institutions can preserve political equality, non-domination, and rule-of-law constraints when probabilistic inference becomes operational authority. Governance that focuses only on accuracy or efficiency mis-specifies the problem, because legitimacy is produced through intelligible reasons, enforceable remedies, and publicly observable accountability.

A coherent typology of AI's political effects can be organized around five mechanism clusters that travel across elections, bureaucracy, platforms, and geopolitics. First, agenda control through attention allocation and ranking reshapes salience, framing, and issue ownership, subtly redistributing political voice without formal censorship. Second, proxy governance through classification distributes eligibility, scrutiny, and opportunity using contestable categories disguised as neutral inference, thereby entrenching informational asymmetries and unequal error burdens. Third, delegation drift through procurement and vendor dependence produces accountability gaps, technological lock-in, and compliance theater, as public institutions outsource core functions without retaining epistemic or auditing capacity. Fourth, behavioral governance through microsegmented persuasion and surveillance feedback shifts influence toward manipulation by reducing publicity and increasing cognitive targeting, weakening the shared informational environments on which democratic deliberation depends. Fifth, strategic instability emerges through security dilemma dynamics, accelerated decision cycles, and epistemic fragility in crisis governance, where automated assessments can amplify misperception and compress opportunities for de-escalation. Each cluster yields actionable governance risks: chilling effects on association, informational discrimination, executive aggrandizement, regulatory capture, and cross-border externalities that resist unilateral solutions.

Submission-ready governance principles follow directly from this institutional diagnosis. Democratic steering requires contestability by design, including enforceable rights to notice, intelligible reasons, and effective remedy for both outcomes and the decision logic that produced them. Transparency must be procedural and operational, requiring decision logs, policy-level objective-function disclosure, documented proxy families, and auditable lifecycle controls that address drift, feedback amplification, and metric gaming. Delegation chains must be re-coupled to responsibility through procurement constraints, interoperability mandates, independent evaluation capacity within the state, and sanctions for non-auditable systems in high-stakes domains. Political equality protections should restrict information discrimination by strengthening publicity conditions for political communication, limiting sensitive-attribute inference, and ensuring traceable targeting rationales. Future conceptual work should refine theories of algorithmic legitimacy, platform constitutionalism, networked sovereignty, and epistemic security, treating AI governance as an ongoing constitutional project under conditions of accelerated, transnational, datafied power.

Declaration of Interest:
No potential conflict of interest was reported by the authors.

Funding Information:
This research did not receive any specific funding from any public, commercial, or non-profit agency.

Disclosure Statement:
No material or relevant stake relating to this research was disclosed by the author(s).

Competing Interest:
No potential conflict of interest was reported by the author(s).

Data Availability Statement:
Data sharing is not applicable to this research article as no new data were created or analysed in this study.

References

- Ahmad, N., Ali, A. W., & Yussof, M. H. B. (2025). The challenges of human rights in the era of artificial intelligence. *UUM Journal of Legal Studies (UUMJLS)*, *16*(1), 150-169.
- Ahmed, S., Wongmahesak, K., Singh, B., & Kumar, S. (2025). Empowering Democratic Processes With AI: Innovations in Voter Engagement, Policy Analysis, and Decision-Making Process. In *Democracy and Democratization in the Age of AI* (pp. 121-132). IGI Global Scientific Publishing.
- Al Lily, M. (2025). The AI president: a country governed by artificial intelligence. *foresight*, *27*(1), 133-146.
- Alcoforado, A., Ferraz, T. P., Bustos, E., Oliveira, A. S., Gerber, R., Santoro, G. L. D. M., ... & Costa, A. H. R. (2024). Augmented democracy: Artificial intelligence as a tool to fight disinformation. *Estudos Avançados*, *38*, 407-426.
- Armiwulan, H., Rahman, R. A., Prabowo, V. N., & HajdÄº, J. (2024). Artificial Intelligence and Its Challenges To Elections In Indonesia: A Legal Analysis. *Jambura Law Review*, *6*(2), 264-285.
- Baele, S. J., Bukhari, I., Whyte, C., Cuomo, S., Jensen, B., Payne, K., & Garcia, E. V. (2024). AI IR: Charting international relations in the age of artificial intelligence. *International Studies Review*, *26*(2), viae013.

- Battista, D. (2024). Political communication in the age of artificial intelligence: an overview of deepfakes and their implications. *Society Register*, *8*(2), 7-24.
- Best, E., Robles, P., & Mallinson, D. J. (2024). The future of AI politics, policy, and business. Business and Politics, 26(2), 171-179.
- Bode, I. (2024). AI Technologies and International Relations: Do We Need New Analytical Frameworks?. *The RUSI Journal*, *169*(5), 66-74.
- Charalabidis, Y., Medaglia, R., & van Noordt, C. (Eds.). (2024). *Research Handbook on Public Management and Artificial Intelligence*. Edward Elgar Publishing.
- Cupać, J., Schopmans, H., & Tuncer-Ebetürk, İ. (2024). Democratization in the age of artificial intelligence: introduction to the special issue. *Democratization*, *31*(5), 899-921.
- Dunleavy, P., & Margetts, H. (2025). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*, *40*(2), 185-214.
- Erman, E., & Furendal, M. (2024). Artificial intelligence and the political legitimacy of global governance. Political Studies, 72(2), 421-441.
- Erskine, T. (2024). AI and the future of IR: Disentangling flesh-and-blood, institutional, and synthetic moral agency in world politics. *Review of International Studies*, *50*(3), 534-559.
- Foos, F. (2024). The use of AI by election campaigns. *LSE Public Policy Review*, *3*(3).
- Ge, J. (2024). Technologies in Peace and Conflict: Unraveling the Politics of Deployment. *Review International Journal of Research Publication and Reviews (IJRPR)*, *5*(5), 5966-5971.
- Gemenis, K. (2024). Artificial intelligence and voting advice applications. *Frontiers in Political Science*, *6*, 1286893.
- Haesevoets, T., Verschuere, B., Van Severen, R., & Roets, A. (2024). How do citizens perceive the use of Artificial Intelligence in public sector decisions?. *Government Information Quarterly*, *41*(1), 101906.
- Haq, E. U., Zhu, Y., Hui, P., & Tyson, G. (2024, May). History in making: Political campaigns in the era of artificial intelligence-generated content. In *Companion Proceedings of the ACM Web Conference 2024* (pp. 1115-1118).
- Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. *Defense & Security Analysis*, *40*(2), 235-269.
- Islam, M. B. E., Haseeb, M., Batool, H., Ahtasham, N., & Muhammad, Z. (2024). AI threats to politics, elections, and democracy: a blockchain-based deepfake authenticity verification framework. *Blockchains*, *2*(4), 458-481.
- Jacobs, J. (2024). The artificial intelligence shock and socio-political polarization. *Technological Forecasting and Social Change*, *199*, 123006.
- Kan, C. H. (2024). Artificial intelligence (ai) in the age of democracy and human rights: normative challenges and regulatory perspectives. *International Journal of Eurasian Education and Culture*, *9*(25), 145-166.
- Kiggins, R. D. (2025). Big data, artificial intelligence, and autonomous policy decision-making: A crisis in international relations theory?. In *The Political Economy of Robots: Prospects for Prosperity and Peace in the Automated 21st Century, 2nd edition* (pp. 297-327). Cham: Springer Nature Switzerland.
- Kretsos, L., Tabaghdehi, S. A. H., & Braganza, A. (2024). The Political Challenge of AI in Modern Society: From National AI Strategy to the Algorithmic Elections. In *Business Strategies and Ethical Challenges in the Digital Ecosystem* (pp. 319-331). Emerald Publishing Limited.
- Łabuz, M., & Nehring, C. (2024). On the way to deep fake democracy? Deep fakes in election campaigns in 2023. *European Political Science*, *23*(4), 454-473.
- Lahdili, N., Önder, M., & Nyadera, I. N. (2024). Artificial intelligence and citizen participation in governance: Opportunities and threats. *Amme İdaresi Dergisi*, *57*(3), 202-229.
- Lemke, N., Trein, P., & Varone, F. (2024). Defining artificial intelligence as a policy problem: A discourse network analysis from Germany. *European Policy Analysis*, *10*(2), 162-187.
- Mahony, S., & Chen, Q. (2025). Concerns about the role of artificial intelligence in journalism, and media manipulation. Journalism, 26(9), 1859-1877.
- Margetts, H., & Dunleavy, P. (2024). The political economy of digital government: How Silicon Valley firms drove conversion to data science and artificial intelligence in public management. *Public Money & Management*, 1-11.
- Marwala, T. (2024). *Mechanism design, behavioral science and artificial intelligence in international relations*. Elsevier.
- Mead, W. R. (2024). The Return of Hamiltonian Statecraft: A Grand Strategy for a Turbulent World. *Foreign Aff.*, *103*, 52.
- Michels, S. (2024). Teaching (with) artificial intelligence: The next twenty years. *Journal of Political Science Education*, *20*(4), 510-521.
- Momeni, M. (2025). Artificial intelligence and political deepfakes: Shaping citizen perceptions through misinformation. *Journal of Creative Communications*, *20*(1), 41-56.
- Nie, M. (2024, May). Artificial Intelligence: The Biggest Threat to Democracy Today?. In Proceedings of the aaai symposium series (Vol. 3, No. 1, pp. 376-379).

- Novelli, C., Formisano, G., Juneja, P., Sandri, G., & Floridi, L. (2024). Artificial Intelligence for the Internal Democracy of Political Parties. *Minds and Machines*, *34*(4), 36.
- Nwosu, C. C., Obalum, D. C., & Ananti, M. O. (2024). Artificial intelligence in public service and governance in Nigeria. *Journal of Governance and Accountability Studies (JGAS)*, *4*(2), 109-120.
- Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.
- Romanishyn, A., Malytska, O., & Goncharuk, V. (2025). AI-driven disinformation: policy recommendations for democratic resilience. *Frontiers in Artificial Intelligence*, *8*, 1569115.
- Scoggins, B., & Robertson, M. P. (2024). Measuring transparency in the social sciences: political science and international relations. *Royal Society Open Science*, *11*(7), 240313.
- Sieber, R., Brandusescu, A., Sangiambut, S., & Adu-Daako, A. (2025). What is civic participation in artificial intelligence?. *Environment and Planning B: Urban Analytics and City Science*, *52*(6), 1388-1406.
- Sienknecht, M., & Vetterlein, A. (2024). Conceptualizing responsibility in world politics. *International Theory*, *16*(1), 26-49.
- Stanger, A., Kraus, J., Lim, W., Millman-Perlah, G., & Schroeder, M. (2024). Terra incognita: the governance of artificial intelligence in global perspective. *Annual Review of Political Science*, *27*(1), 445-465.
- Subekti, D., Yusuf, M., Saadah, M., & Wahid, M. (2025). Social media and disinformation for candidates: The evidence in the 2024 Indonesian presidential election. *Frontiers in Political Science*, *7*, 1625535.
- Tosi, D., Chiappa, M., & Pizzul, D. (2025). AI chatbots in political campaigns: A practical experience in the EU's 2024 parliament elections. *Social Science Computer Review*, 08944393251320063.
- Volkivskyi, M., Islam, T., Ness, S., & Mustafa, B. (2024). The Impact of Machine Learning on the Proliferation of State-Sponsored Propaganda and Implications for International Relations. *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)*, *2*(2), 17-24.
- Wadipalapa, R. P., Katharina, R., Nainggolan, P. P., Aminah, S., Apriani, T., Ma'rifah, D., & Anisah, A. L. (2024). An ambitious artificial intelligence policy in a decentralised governance system: evidence from Indonesia. *Journal of Current Southeast Asian Affairs*, *43*(1), 65-93.
- Walker, C. P., Schiff, D. S., & Schiff, K. J. (2024, March). Merging AI incidents research with political misinformation research: introducing the political Deepfakes incidents database. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 38, No. 21, pp. 23053-23058).
- Walter, Y. (2024). Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*, *4*(1), 14.
- Wei, Z., Xu, X., & Hui, P. (2024, May). Digital democracy at crossroads: A meta-analysis of web and ai influence on global elections. In *Companion Proceedings of the ACM Web Conference 2024* (pp. 1126-1129).
- Wong, W. (2025). Trends in Political Science Research: Artificial Intelligence and Voter Disinformation. *International Political Science Abstracts*, *75*(2), 205-222.
- Yigitcanlar, T., David, A., Li, W., Fookes, C., Bibri, S. E., & Ye, X. (2024). Unlocking artificial intelligence adoption in local governments: Best practice lessons from real-world implementations. *Smart Cities*, *7*(4), 1576-1625.
- Zidouemba, M. T. (2025). Governance and artificial intelligence: the use of artificial intelligence in democracy and its impacts on the rights to participation. *Discover Artificial Intelligence*, *5*(1), 12.

© 2026, Author(s).

This open access publication is distributed under Creative Commons Attribution (CC BY-NC-SA 4.0) License.

You are free to:
Share — copy and redistribute the material in any medium or format.
Adapt — remix, transform, and build upon the material.

However,
Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made.
Non-Commercial — You may not use the material for commercial purposes.
Share Alike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license.

You shall not apply legal terms or technological measures that legally restrict others from doing anything the license permits.
There are no additional restrictions.