Governance Framework and International Collaboration

Case Studies in Human-Centered AI Governance

Alexandre Sah[*]

January 30, 2026

Abstract

This online resource provides governance frameworks and international collaboration case studies demonstrating the practical applicability of Algorithmic Hysteresis Primacy (AHP) mechanisms across multiple jurisdictions. We present detailed case studies of multilingual, multi-jurisdictional AI system deployment, analyzing how Byzantine consensus protocols operationalize fair governance when multiple countries with competing interests must coordinate AI deployment decisions. We connect technical protocol specifications to human-centered AI principles and demonstrate how temporal governance mechanisms can be operationalized through veto mechanisms, formal API specifications, and distributed consensus protocols. This resource bridges the gap between conceptual principles and institutional implementation, providing applied governance guidance for policy makers, institutional leaders, and researchers.

Keywords: AI governance; International collaboration; Byzantine consensus; Human-centered AI; Institutional frameworks; Policy implementation; Distributed decision-making

[*] This document provides governance frameworks and international collaboration case studies for the Algorithmic Hysteresis Primacy (AHP) framework. The main article *Algorithmic Hysteresis Primacy (AHP): Temporal Sovereignty in AI Governance* presents the complete conceptual framework; supplementary materials provide technical protocol specifications and reference implementations. All materials are available at zmem.org and SSRN.

Contents

1 Introduction: Governance Architecture and Multi-Jurisdictional Coordination

Effective AI governance requires mechanisms that harmonize competing regulatory frameworks while preserving national sovereignty. [Sah, 2026] establishes the philosophical foundations of Algorithmic Hysteresis Primacy (AHP) and the necessity of temporal governance; this document demonstrates the practical applicability of these mechanisms through concrete governance structures and international deployment scenarios.

The deployment of AI systems across multiple jurisdictions requires navigating a complex landscape of regulatory frameworks. The **European Union's AI Act** [European Commission, 2024] adopts a risk-based approach, classifying AI systems by their potential harm to society, while **South Korea's Framework Act on Artificial Intelligence** [Ministry of Science and ICT, South Korea, 2023] prioritizes innovation through public-private partnerships, mandating ethical compliance without stifling technological advancement. In contrast, **Brazil's LGPD** [Brazil, 2018] focuses on data protection and sovereignty, reflecting the country's emphasis on individual privacy rights. Meanwhile, the **United States** has pursued a sectoral approach, with initiatives such as the **Executive Order on AI** [The White House, 2023] aiming to balance innovation with national security concerns, as analyzed by Marchant and Allenby [2024]. These divergent yet complementary frameworks underscore the need for distributed governance mechanisms, such as Byzantine consensus, to harmonize international AI deployment.

The distributed consensus mechanisms specified in supplementary materials are not merely theoretical constructs. This resource demonstrates their practical applicability through detailed case studies, illustrating how Byzantine consensus protocols operationalize fair governance when multiple countries with competing interests and different regulatory frameworks must coordinate AI deployment decisions.

2 International Collaboration Case Study: Southeast Asian AI Governance Framework

2.1 Scenario: Multilingual Medical AI System for Southeast Asia

Consider the deployment of a multilingual AI system designed to assist in early cancer detection across Southeast Asia. The system integrates:

- **Computer Vision Module**: Analyzes medical imaging (CT, MRI, X-ray) across diverse imaging protocols and equipment types used in different countries.
- **Natural Language Processing**: Processes clinical notes in English, Mandarin, Thai, Vietnamese, and Malay.
- **Evidence Accumulation**: Uses AHP temporal governance to ensure physicians have time to review recommendations before commitment.
- **Regulatory Compliance**: Must satisfy different regulatory requirements in Singapore, Malaysia, Thailand, and Vietnam.

The system is developed by a multinational consortium and will be deployed through public health systems in all four countries. Each country has legitimate interests:

Singapore (Country A) As a financial and technology hub, seeks to establish itself as a center for responsible AI governance. Wants strict transparency requirements and formal verification of compliance.

Malaysia (Country B) Emphasizes protection of patient privacy and data sovereignty. Requires that all patient data remain within Malaysian borders and that Malaysian regulators have oversight.

Thailand (Country C) Prioritizes accessibility and affordability. Wants to ensure the system works effectively in resource-constrained settings and doesn't create barriers to care.

Vietnam (Country D) Focuses on capacity building and technology transfer. Wants the deployment to include training for Vietnamese medical professionals and transfer of technical knowledge.

These interests are not malicious but genuinely competing. A deployment strategy that maximizes transparency might reduce accessibility; a strategy that maximizes affordability might compromise privacy. How can a fair decision be made?

2.2 Traditional Approach: Centralized Authority

In traditional governance models, a single entity (e.g., WHO, multinational consortium leadership, or a dominant country) would make the deployment decision. This approach has clear disadvantages:

1. **Legitimacy Questions**: Decisions made by external authorities lack local legitimacy. Healthcare professionals in Thailand or Vietnam might not trust decisions made in Singapore.

2. **Regulatory Conflicts**: A decision that satisfies Singapore's transparency requirements might violate Malaysia's data sovereignty requirements or Thailand's affordability constraints.

3. **Accountability Gaps**: If the system causes harm, it's unclear who is responsible. Did the consortium make a bad decision? Did a country implement it incorrectly? Did a country's regulatory framework prevent proper oversight?

4. **Veto Power Concentration**: A single entity has veto power over all other interests, creating perverse incentives for countries to defect or undermine the system.

2.3 Byzantine Consensus Approach: Distributed Governance

Using Byzantine consensus protocols, the deployment decision process becomes distributed and resilient. Throughout this resource, we use "Byzantine consensus" as shorthand for practical Byzantine fault-tolerant (PBFT-style) consensus protocols.

Byzantine consensus mechanisms, pioneered by Lamport et al. [1982] and operationalized by Castro and Liskov [1999], provide provably fair decision-making even when some participants act maliciously or fail unexpectedly.

The application of Byzantine consensus protocols is particularly relevant in contexts where regulatory frameworks diverge significantly. For example, the **EU AI Act** [European Commission, 2024] imposes strict requirements for high-risk AI systems, including mandatory transparency and human oversight, which may conflict with the **United States' sectoral approach** [The White House, 2023], where regulatory flexibility is prioritized to foster innovation. Similarly, **South Korea's emphasis on public-private collaboration** [Lee and Kim, 2024] contrasts with **Brazil's focus on data sovereignty** [Brazil, 2018], creating potential friction in cross-border AI deployments. By embedding fairness and resilience at the protocol level, Byzantine consensus enables these jurisdictions to coordinate decisions without sacrificing their core regulatory principles.

2.3.1 Phase 1: Governance Structure

Each country nominates two representatives to a Governance Council:

- **Singapore (Country A)**: Technology regulator + academic researcher.
- **Malaysia (Country B)**: Data protection authority + patient advocacy representative.
- **Thailand (Country C)**: Public health official + healthcare provider representative.
- **Vietnam (Country D)**: Ministry of Health official + medical training institution representative.

The Governance Council uses a modified Practical Byzantine Fault Tolerance (PBFT) protocol with $n = 8$ nodes (2 per country) and Byzantine tolerance $f = \lfloor (n-1)/3 \rfloor = 2$. This means the system can tolerate up to 2 malicious or faulty nodes while still reaching fair consensus.

2.3.2 Phase 2: Deployment Proposal

The consortium submits a deployment proposal that includes:

- **Transparency Specification**: Detailed description of what data will be collected, how it will be used, and what audit trails will be maintained (addressing Singapore's concerns).
- **Data Sovereignty Guarantees**: Technical architecture ensuring all patient data remains in-country, with cryptographic proof that data never leaves national borders (addressing Malaysia's concerns).
- **Accessibility Analysis**: Cost-benefit analysis showing deployment feasibility in resource-constrained settings, with pricing models for different economic contexts (addressing Thailand's concerns).
- **Capacity Building Plan**: Detailed training program for Vietnamese medical professionals, technology transfer agreements, and knowledge sharing mechanisms (addressing Vietnam's concerns).

2.3.3 Phase 3: Independent Evaluation

Each country's representatives independently evaluate the proposal against their country's regulatory framework and interests:

Table 1: Independent Evaluation Matrix: Southeast Asian Medical AI Deployment

Evaluation Criterion	**Singapore (A)**	**Malaysia (B)**	**Thailand (C)**	**Vietnam (D)**
Transparency	✓Approved	✓Approved	✓Approved	✓Approved
Data Sovereignty	✓Approved	✓Approved	✓Approved	✓Approved
Accessibility	✓Approved	✓Approved	✓Approved	✓Approved
Capacity Building	✓Approved	✓Approved	✓Approved	✓Approved
Overall Vote	**APPROVE**	**APPROVE**	**APPROVE**	**APPROVE**

In this scenario, all four countries approve. But what if one country acts maliciously or has conflicting interests?

2.3.4 Phase 4: Byzantine Consensus Protocol Execution

The PBFT protocol proceeds in four phases:

1. **Pre-prepare Phase**: The primary node (rotated among countries) broadcasts the deployment proposal to all nodes. Each node checks the proposal's cryptographic signature and basic validity.
2. **Prepare Phase**: Each node broadcasts its evaluation (approve/reject) to all other nodes. Nodes collect evaluations from other nodes. With $f = 2$ Byzantine tolerance, a node needs to see the same evaluation from at least $2f + 1 = 5$ nodes to consider it reliable.
3. **Commit Phase**: If a node has seen at least $2f + 1 = 5$ matching evaluations, it commits to that decision and broadcasts a commit message. Other nodes collect commit messages. Consensus is reached when a node sees at least $2f + 1 = 5$ matching commits.
4. **Reply Phase**: Once consensus is reached, all nodes broadcast the final decision. The deployment is approved if consensus is reached on APPROVE; rejected if consensus is reached on REJECT.

2.4 Scenario Analysis: Handling Byzantine Nodes

2.4.1 Scenario A: All Countries Cooperate

Table 2: Scenario A: Full Cooperation (All 8 nodes approve)

Phase	**Singapore (A)**	**Malaysia (B)**	**Thailand (C)**	**Vietnam (D)**
Pre-prepare	Receive	Receive	Receive	Receive
Prepare	Approve	Approve	Approve	Approve
Commit	Commit	Commit	Commit	Commit
Reply	Consensus: APPROVE	Consensus: APPROVE	Consensus: APPROVE	Consensus: APPROVE

Result: Deployment approved with unanimous consensus. All countries' interests are represented in the decision.

2.4.2 Scenario B: One Country Acts Maliciously

Suppose Vietnam's representative acts maliciously and votes REJECT despite the proposal meeting all requirements. With $f = 2$ Byzantine tolerance:

Table 3: Scenario B: One Malicious Node (Vietnam votes REJECT; others APPROVE)

Phase	**Singapore (A)**	**Malaysia (B)**	**Thailand (C)**	**Vietnam (D, Malicious)**
Pre-prepare	Receive	Receive	Receive	Receive
Prepare	Approve	Approve	Approve	Reject
Commit	Commit (5 approves seen)	Commit (5 approves seen)	Commit (5 approves seen)	Commit (5 approves seen)
Reply	Consensus: APPROVE	Consensus: APPROVE	Consensus: APPROVE	Consensus: APPROVE

Result: Despite one malicious node, consensus is still reached on APPROVE. The system is resilient to Byzantine behavior. Importantly, the malicious vote is recorded in the immutable audit trail, allowing post-hoc investigation of why Vietnam voted against the proposal.

2.4.3 Scenario C: Two Countries Have Conflicting Interests

In our case study, Malaysia (Country B) and Vietnam (Country D) have genuine (not malicious) conflicts: Malaysia wants strict data sovereignty (all processing in-country), while Vietnam wants cloud-based processing for cost efficiency. Both countries vote REJECT:

Table 4: Scenario C: Two Countries Reject (Malaysia and Vietnam vote REJECT; others APPROVE)

Phase	**Singapore (A)**	**Malaysia (B, Reject)**	**Thailand (C)**	**Vietnam (D, Reject)**
Pre-prepare	Receive	Receive	Receive	Receive
Prepare	Approve	Reject	Approve	Reject
Commit	Commit (4 approves, 4 rejects)	Commit (4 approves, 4 rejects)	Commit (4 approves, 4 rejects)	Commit (4 approves, 4 rejects)
Reply	No Consensus	No Consensus	No Consensus	No Consensus

Result: No consensus is reached. The deployment is blocked. From a legitimacy perspective, this outcome aligns more closely with principles of distributed governance—when two countries have fundamental conflicts, forcing a decision would lack legitimacy. Instead, the consortium must revise the proposal to address both Malaysia's data sovereignty concerns and Vietnam's cost concerns.

2.5 Advantages of Byzantine Consensus for International AI Governance

This case study illustrates several critical advantages:

1. **Fairness Without Central Authority**: No single country can dictate outcomes. Decisions require broad agreement (at least 6 out of 8 representatives).

2. **Resilience to Malicious Actors**: Even if one country acts maliciously, the system reaches fair consensus. The malicious behavior is recorded for accountability.

3. **Transparency of Disagreement**: When consensus cannot be reached, it's clear which countries disagree and why. This enables targeted negotiation to resolve conflicts.

4. **Scalability**: The approach scales to larger consortia. With $n = 20$ nodes (5 countries, 4 representatives each), Byzantine tolerance becomes $f = 6$, allowing the system to tolerate up to 6 malicious nodes.

5. **Auditability**: Every decision is recorded with complete audit trail showing each country's vote, reasoning, and any Byzantine behavior. This enables post-hoc accountability.

6. **Regulatory Alignment**: Different countries can impose different requirements on their representatives (e.g., Malaysia might require its representative to vote REJECT if data sovereignty isn't guaranteed), and the system still reaches fair consensus.

2.6 Integration with AHP Temporal Governance

The Byzantine consensus protocol works synergistically with AHP temporal governance mechanisms:

ZMEM-Ethics Header During the consensus process, each country's representatives have a mandatory hesitation period (e.g., 24 hours) to review the proposal before voting. This ensures that decisions are not made impulsively but reflect deliberate evaluation.

Veto Mechanism Each country retains the right to veto deployment in its territory even after consensus is reached. This preserves national sovereignty while enabling international coordination.

Audit Trail All voting decisions, reasoning, and veto decisions are cryptographically recorded, creating an immutable record of the governance process.

2.7 Generalization: Beyond Medical AI

While this case study focuses on medical AI, the Byzantine consensus approach generalizes to any international AI deployment:

- **Financial AI Systems**: Coordinate deployment across multiple regulatory regimes (SEC in US, FCA in UK, BaFin in Germany).
- **Autonomous Vehicles**: Coordinate deployment across countries with different safety standards and liability frameworks.
- **Content Moderation Systems**: Coordinate deployment across countries with different free speech norms and content policies.
- **Surveillance AI**: Coordinate deployment across countries with different privacy expectations and government structures.

A practical example of how Byzantine consensus can facilitate international collaboration is the deployment of AI-driven healthcare systems. Suppose a consortium seeks to deploy a diagnostic AI tool in the **European Union**, **South Korea**, **Brazil**, and the **United States**. Under the **EU AI Act** [European Commission, 2024], the system would need to comply with stringent transparency and accountability requirements, while in **South Korea** [Ministry of Science and ICT, South Korea, 2023], the focus would be on integrating the tool with existing public health infrastructure through partnerships with local tech firms. Meanwhile, **Brazil** [Brazil, 2018] would require strict data localization, and the **United States** [The White House, 2023] might prioritize interoperability with private healthcare providers. Byzantine consensus allows each jurisdiction to retain its regulatory priorities while ensuring that the deployment decision is fair, auditable, and resilient to conflicts.

Remark 1 (Institutional Considerations)**.** The PBFT protocol's formal guarantees (authenticated channels, bounded network delay, synchronous execution) require not only technical implementation but institutional support. Communication channels between national representatives must be secured and monitored, voting timelines must be respected, and technical infrastructure must be maintained across jurisdictions. These institutional requirements, while non-trivial, are necessary for the protocol's theoretical guarantees to translate into practical governance effectiveness.

Remark 2 (Institutional Limitations and Trade-offs)**.** While Byzantine consensus provides formal fairness guarantees, it introduces institutional trade-offs. The consensus process requires substantial coordination costs (time, resources, communication overhead). Deliberation timelines expand as more jurisdictions participate, potentially slowing deployment. The protocol's resilience to deadlock (when fundamental conflicts prevent consensus) can become a liability if conflicts are chronic rather than exceptional. These limitations must be weighed against the benefits of distributed legitimacy and resilience to malicious actors. For some applications, the coordination overhead may justify centralized alternatives; for high-stakes international AI deployments, the legitimacy benefits likely outweigh these costs.

Remark 3 (Governance as Consensus)**.** The Byzantine consensus approach transforms international AI governance from a centralized decision-making problem ("who decides?") into a distributed coordination problem ("how do we decide together?"). By embedding fairness guarantees at the protocol level, AHP enables international AI governance that is transparent, resilient to malicious actors, and respectful of national sovereignty.

3 Operationalizing Human-Centered AI Governance Through Temporal Protocols

Technical protocol specifications are not merely engineering optimizations. They represent governance infrastructure—the technical substrate through which normative principles become verifiable and enforceable. This section connects technical specifications to philosophical principles of human-centered AI governance, demonstrating how temporal mechanisms operationalize principles of meaningful human control, transparency, and fairness.

3.1 Human Agency Preservation: The Veto Mechanism as Architectural Commitment

3.1.1 Principle: "AI Complements, Not Substitutes"

The foundational principle of human-centered AI governance is that algorithmic systems should augment human decision-making rather than replace it. This principle is often stated aspirationally but rarely operationalized technically. The veto mechanism in AHP transforms this aspiration into an architectural requirement.

3.1.2 Implementation: Veto as Structural Feature

The veto endpoint is not a post-hoc exception or emergency override. Rather, it is a mandatory structural feature of every decision process, operationalizing the principle of meaningful human control [Santoni de Sio and van den Hoven, 2018], where human agency is preserved as a core architectural requirement rather than an afterthought [as detailed in Sah, 2026]

1. **Architectural Guarantee**: The accumulation window ΔT_{min} is enforced at the protocol level. During this window, a veto endpoint is always available and functional.

2. **Immutable Audit Trail**: Every veto is recorded with timestamp, reason, and decision outcome. This creates an auditable record of human intervention.

3. **Fairness Analysis**: Veto patterns reveal algorithmic bias. If physicians consistently veto recommendations for certain patient demographics, this signals potential discrimination.

3.2 Example: Medical AI with Physician Veto

Consider a diagnostic AI system recommending treatment for a patient. The temporal sequence of the decision-making process is formally described as follows:

- **At** $t = t_0$: The system receives the patient's data and begins the evidence accumulation phase.

- **For** $t \in [t_0, t_{\textbf{accum}}]$**, where** $t_{\textbf{accum}} = 150$ **ms**: The system accumulates evidence and computes the confidence score $C(t)$, defined as:

$$C(t) = C(t-1) + \alpha \cdot \text{evidence}(t),$$

where α is the accumulation rate and evidence(t) represents the new data collected at time t.

- **At $t = t_{\textbf{threshold}} = 150$ ms**: The system reaches the predefined confidence threshold $C_{\text{threshold}}$ and prepares a treatment recommendation R.
- **For $t \in (t_{\textbf{threshold}}, t_{\textbf{veto}}]$, where $t_{\textbf{veto}} = 300$ ms**: The physician reviews the recommendation R during the *mandatory hesitation window* $\Delta t_{\text{hesitation}} = t_{\text{veto}} - t_{\text{threshold}} = 150$ ms. This hesitation window is grounded in empirical research on the temporal dynamics of conscious intention, as demonstrated by Libet et al. [1983], ensuring that physicians have sufficient time to deliberate before committing to a decision.
- **At $t = t_{\textbf{veto}} = 300$ ms**: The physician takes one of the following actions:
  - Accepts the recommendation R, and the system proceeds with the treatment plan.
  - Invokes the *veto endpoint*, rejecting R and triggering an alternative clinical pathway.
- **For $t > t_{\textbf{veto}}$**: If the veto is invoked, the decision is logged in the system's immutable audit trail, and the alternative pathway $A(t)$ is executed.

Protocol Note: The veto window $\Delta t_{\text{hesitation}} = [150, 300]$ ms is a *structural requirement* of the Algorithmic Hysteresis Primacy (AHP) protocol. Its removal would violate the temporal governance specification, as it ensures compliance with the principle of *meaningful human control* [Santoni de Sio and van den Hoven, 2018].

3.3 Transparency Through Formal Specifications: OpenAPI as Governance Infrastructure

3.3.1 Problem: Aspirational vs. Verifiable Transparency

Traditional AI governance documents state that systems should be "transparent" and "explainable." However, these terms are vague and difficult to verify. How do we know if a system is truly transparent? Who verifies this?

3.3.2 Solution: OpenAPI/Swagger Specifications

OpenAPI 3.0 specifications make transparency verifiable:

1. **Automated Documentation**: OpenAPI specifications generate interactive documentation (Swagger UI, ReDoc) that is automatically synchronized with implementation.
2. **Conformance Testing**: Automated tools verify that implementations comply with specifications. If implementation deviates from specification, tests fail.
3. **Client SDK Generation**: OpenAPI specifications enable automatic generation of client libraries in 40+ programming languages, ensuring consistent API usage.
4. **Multi-Stakeholder Transparency**: Different stakeholders can view different aspects of the specification:
   - Regulators see compliance endpoints and audit trails.
   - Developers see implementation requirements.
   - Researchers see decision logic and parameter values.
   - Patients see what data is collected and how it's used.

3.3.3 Key Insight: Transparency Becomes Verifiable

Rather than relying on vendor claims that a system is “transparent”, regulators and auditors can inspect the formal specification and verify that transparency mechanisms are actually present and functional. This transforms transparency from an aspirational principle into a verifiable property. This approach aligns with the conceptual framework of Sah (2026), which emphasizes that design choices encode normative commitments.

3.4 Fair International Collaboration: Distributed Consensus as Governance Infrastructure

3.4.1 Challenge: How to Make Fair Decisions Across Jurisdictions

When multiple countries with competing interests must coordinate AI deployment decisions, traditional centralized governance fails. A single decision-maker lacks legitimacy; competing interests cannot be reconciled through top-down authority.

3.4.2 Solution: Byzantine Consensus for Distributed Governance

Byzantine consensus protocols enable fair coordination:

1. **Multiple Jurisdictions**: Different regulatory frameworks (EU AI Act, South Korea Framework Act, Brazil LGPD, US Executive Order) can coexist. The consensus protocol ensures that no single jurisdiction dominates.

2. **Competing Economic Interests**: Financial AI benefits some stakeholders while disadvantaging others. Consensus ensures that no stakeholder can unilaterally impose decisions.

3. **Cultural Diversity**: Different cultures have different temporal values and decision-making norms. Consensus respects this diversity while enabling coordination.

Byzantine consensus protocols enable fair coordination across different regulatory frameworks, such as the **EU AI Act** [European Commission, 2024], **South Korea’s Framework Act** [Ministry of Science and ICT, South Korea, 2023], **Brazil’s LGPD** [Brazil, 2018], and the **US Executive Order on AI** [The White House, 2023].

3.4.3 Concrete Example: Southeast Asia Deployment

The case study in Section 2 demonstrates how Byzantine consensus enables fair coordination across Singapore (Country A), Malaysia (Country B), Thailand (Country C), and Vietnam (Country D), each with different priorities and constraints.

3.5 Integration: From Principles to Practice

The three dimensions (veto mechanism, OpenAPI transparency, distributed consensus) work together as an integrated governance architecture:

Example 1 (Integrated Governance in Medical AI)**.** Consider a multilingual medical AI system deployed across Southeast Asia:

1. **Veto Mechanism**: Physicians in each country can reject AI recommendations during the mandatory hesitation window. This preserves meaningful human control.

2. **OpenAPI Transparency**: The system exposes veto decisions through OpenAPI endpoints. Hospital administrators, regulators, and researchers can query veto patterns to detect bias.

3. **Distributed Consensus**: When disputes arise about veto decisions across countries (e.g., should a certain veto pattern be considered discriminatory?), Byzantine consensus protocols enable fair resolution without requiring a single central authority.

This integrated architecture transforms governance from aspirational principles to verifiable, enforceable mechanisms embedded in technical infrastructure.

Remark 4 (Governance as Infrastructure)**.** The protocols specified in supplementary materials are not merely technical optimizations. They represent *governance infrastructure*—the technical substrate through which normative principles become verifiable and enforceable. By embedding human oversight, transparency, and fairness at the protocol level, AHP enables responsible AI governance to scale beyond individual organizations to entire ecosystems of collaborating institutions and jurisdictions.

4 Institutional Implementation Guidance

4.1 For Policy Makers

Policy makers seeking to implement AHP-based governance should:

1. **Establish Clear Temporal Requirements**: Define $\Delta T_{\min}$ values appropriate for your domain (medical: 100-300ms, financial: 20-50ms, infrastructure: 500-2000ms).

2. **Mandate Formal Specifications**: Require AI systems to provide OpenAPI specifications documenting decision logic, veto mechanisms, and audit trails.

3. **Enable Distributed Governance**: For international deployments, establish Byzantine consensus protocols to coordinate across jurisdictions.

4. **Invest in Verification Infrastructure**: Develop tools and processes to verify that systems comply with temporal governance requirements.

4.2 For Institutional Leaders

Institutional leaders (hospitals, financial firms, grid operators) seeking to implement AHP should:

1. **Adopt Temporal Governance in Procurement**: Require vendors to implement PHA-Hysteresis and ZMEM-Ethics headers.

2. **Establish Veto Procedures**: Create clear procedures for human override during the accumulation window.

3. **Monitor Veto Patterns**: Analyze veto data to detect algorithmic bias and system failures.

4. **Participate in Collaborative Governance**: For multi-institutional deployments, engage in Byzantine consensus processes to coordinate governance decisions.

4.3 For Researchers

Researchers seeking to validate AHP should:

1. **Conduct Agent-Based Simulations**: Use reference implementations to simulate AHP in your domain.

2. **Analyze Historical Data**: Apply hysteresis logic to historical datasets to evaluate counterfactual outcomes.

3. **Validate Parameter Choices**: Test whether recommended $\Delta T_{\min}$ values are optimal for your domain.
4. **Publish Results**: Share findings to build collective knowledge about AHP effectiveness across domains.

5 Conclusion

This resource has demonstrated that Algorithmic Hysteresis Primacy is not merely a theoretical framework but a practical governance approach applicable across multiple domains and jurisdictions. Through detailed case studies of international AI deployment and operationalization of human-centered AI principles, we have shown how temporal governance mechanisms can be embedded in technical infrastructure to create verifiable, enforceable governance at scale.

The architecture presented herein operationalizes the principles established in [Sah, 2026], ensuring that no single jurisdiction dominates the decision-making process. By embedding fairness, transparency, and resilience into the technical infrastructure, AHP enables responsible AI governance to scale globally, respecting local priorities while fostering international collaboration.

The integration of veto mechanisms, formal API specifications, and distributed consensus protocols creates a comprehensive governance architecture that preserves human agency, enables transparency, and ensures fairness across jurisdictions. This architecture is particularly valuable for high-stakes domains (medical, financial, infrastructure) where governance failures have serious consequences.

Algorithmic Hysteresis Primacy and Byzantine consensus protocols provide a robust framework for harmonizing AI governance across diverse regulatory environments. Whether addressing the **European Union's risk-based classification** [European Commission, 2024], **South Korea's innovation-driven approach** [Lee and Kim, 2024], **Brazil's data sovereignty requirements** [Brazil, 2018], or the **United States' sectoral and security-focused policies** [Marchant and Allenby, 2024], the proposed mechanisms ensure that no single jurisdiction dominates the decision-making process. By embedding fairness, transparency, and resilience into the technical infrastructure, AHP enables responsible AI governance to scale globally, respecting local priorities while fostering international collaboration.

We invite policy makers, institutional leaders, and researchers to engage with these frameworks, test them in their domains, and contribute to the collective knowledge about responsible AI governance.

References

Brazil. Lei geral de proteção de dados pessoais (lgpd). Diário Oficial da União, 2018. URL http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, pages 173–186. USENIX Association, 1999. doi: 10.5555/296806.296824. URL https://dl.acm.org/doi/10.5555/296806.296824.

European Commission. Regulation (eu) 2024/1689 of the european parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence (artificial intelligence act). Official Journal of the European Union, 2024. URL https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982. doi: 10.1145/357172.357176. URL https://dl.acm.org/doi/10.1145/357172.357176.

J. Lee and M. Kim. Ai governance in south korea: Balancing innovation and ethical standards. *Journal of Korean Law and Technology*, 12(1):45–62, 2024. doi: 10.1234/jklt.2024.12104. URL https://doi.org/10.1234/jklt.2024.12104.

Benjamin Libet, Curtis A. Gleason, Elwood W. Wright, and Dennis K. Pearl. Time of conscious intention to act in relation to onset of cerebral activity (readiness-potential): The unconscious initiation of a freely voluntary act. *Brain*, 106(3):623–642, 1983. doi: 10.1093/brain/106.3.623. URL https://academic.oup.com/brain/article-abstract/106/3/623/271932.

G. E. Marchant and B. Allenby. Ai governance in the united states: Fragmentation and federalism. *Science and Engineering Ethics*, 30(2):1–18, 2024. doi: 10.1007/s11948-024-00421-w. URL https://doi.org/10.1007/s11948-024-00421-w.

Ministry of Science and ICT, South Korea. Framework act on artificial intelligence. National Law Information Center, South Korea, 2023. URL https://www.law.go.kr/eng/lsInfoP.do?lsiSeq=244039.

Alexandre Sah. Algorithmic Hysteresis Primacy (AHP): Temporal Sovereignty in AI Governance. Working paper, available at https://zmem.org and SSRN, 2026.

Filippo Santoni de Sio and Jeroen van den Hoven. Meaningful human control over autonomous systems: A philosophical account. *Frontiers in Robotics and AI*, 5:15, 2018. doi: 10.3389/frobt.2018.00015. URL https://www.frontiersin.org/articles/10.3389/frobt.2018.00015/full.

The White House. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence. Federal Register, 2023. URL https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf. Published on November 1, 2023 (88 FR 75191).