EPINOVA–2026–PB–58

Policy Brief

Series Information:
This policy brief is part of the EPINOVA Policy Brief Series on Strategic Competition, AI-Enabled Warfare, and Information Conflict.

Beyond Model Capability:

A System-Level Framework for AI Power

Author: Shaoyuan Wu

Affiliation: Global AI Governance and Policy Research Center, EPINOVA LLC

Date: June 25, 2026

Recommended Citation:
Wu, Shaoyuan (2026), *Beyond Model Capability: A System-Level Framework for AI Power*, Policy Brief No. EPINOVA–2026–PB–58, Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.67037/epinova.pb.2026.058

GLOBAL AI GOVERNANCE
RESEARCH CENTER

EPINOVA

Key Judgments

- **Model capability is necessary but insufficient.** Benchmarks, parameter scale, and public adoption measure visible performance, but not real-world AI power.
- **Data quality is a core source of advantage.** Rare, verified, proprietary, domain-specific, and experience-based data can create advantages that public rankings do not capture.
- **Resource access turns capability into operational influence.** AI systems connected to compute, capital, infrastructure, sensors, platforms, labor, robotics, or physical assets can move beyond information processing.
- **Authority determines how capability is released.** The same model may be constrained in public use, expanded in enterprise settings, or operationalized under governmental, military, or emergency authorization.
- **Interfaces convert analytical capability into operational action.** AI becomes more consequential when it can trigger actions, allocate resources, adjust operations, influence decisions, or alter system states.
- **Rule space determines how AI power is constrained or released.** Law, institutional policy, platform governance, national security exceptions, emergency powers, and gray-zone conditions shape what AI systems are allowed, restricted, or enabled to do.

Executive Summary

AI competition and capability are often assessed through model performance, benchmark rankings, parameter scale, public adoption, or user reach. These indicators are useful, but they capture only the visible layer of AI capability.

In this brief, AI power refers to the capacity of an AI system to shape decisions, mobilize resources, influence behavior, or alter real-world outcomes within a specific institutional, operational, and rule environment.

This policy brief argues that AI power depends not only on model capability, but also on data quality, resource access, authority, real-world interfaces, and rule space. A public-facing model may be highly capable but operationally constrained, while a narrower system may have greater real-world impact if it is embedded in institutions, infrastructure, financial systems, or exceptional legal, institutional, or operational environments.

The central argument is that AI power is not reducible to model intelligence. It is produced by the broader system that determines what the system can know, access, mobilize, do under authorization, and change.

Policy Brief

Why This Matters

AI competition is often described as a race among models. This framing is too narrow. The most consequential AI systems may not be the most visible public-facing models, but the systems most deeply connected to data, infrastructure, authority, and real-world operations.

This matters for policy because governance focused only on public-facing outputs may miss where AI power is actually formed. The more important question is not only what an AI model can say, but what it can access, influence, do under authorization, and change.

A system-level view of AI power can help policymakers, firms, and researchers better identify where AI creates strategic advantage, operational risk, market concentration, or institutional dependency.

Analytical Note

This brief uses AI power as an analytical concept rather than a conventional technical benchmark. The concept is intended to capture how AI capability becomes consequential once it is connected to data, resources, authority, interfaces, and rule conditions. It therefore shifts attention from the isolated model to the broader AI power system in which the model is trained, authorized, connected, and deployed.

The proposed expression should be read first as a structural model. Its purpose is to identify the key variables that shape real-world AI influence and to show why model capability alone is an incomplete measure. When operationalized as an AI System Power Index, the framework can support comparative assessment, but such measurement requires explicit assumptions about normalization, weighting, sectoral context, and available evidence.

1. Existing Measurement Landscape and the Limits of Model Rankings

Existing indices already measure important aspects of AI development. The Stanford AI Index tracks technical performance, investment, adoption, infrastructure, governance, and responsible AI trends (AI Index Steering Committee, 2026). The Global AI Index ranks national AI capacity across implementation, innovation, and investment (Tortoise Media, 2024). The Government AI Readiness Index evaluates public-sector readiness to use AI (Oxford Insights, 2025). Emerging work on AI power disparity has also begun to examine how power is distributed among actors in the AI ecosystem (Kim et al., 2025).

These efforts provide important building blocks, but they do not fully measure AI power at the system level. Most existing frameworks focus on model capability, national capacity, government readiness, infrastructure, governance maturity, or actor-level power disparities (AI Index Steering Committee, 2026; Kim et al., 2025; Oxford Insights, 2025; Tortoise Media, 2024). They do not directly assess how a particular AI system becomes consequential through the interaction of model capability, data quality, resource access, authority, real-world interfaces, and rule space.

This gap matters because public debate on AI competition still relies heavily on visible indicators such as benchmark scores, model rankings, parameter counts, chatbot performance, and user adoption. These measures show how well a model performs under evaluated conditions, but not how much influence it can exercise once embedded in institutions, infrastructure, markets, or state functions.

This brief therefore treats AI power not as a single technical capability, national readiness score, or actor-level power disparity, but as a system-level condition: the degree to which AI capability is connected to what the system can know, access, mobilize, do under authorization, and change.

2. A Conceptual and Quantifiable Framework for AI Power

A more complete expression of AI power can be stated as:

$$\boldsymbol{AI\ Power} = f(\boldsymbol{model\ capability}, \boldsymbol{data\ quality}, \boldsymbol{resource\ access}, \boldsymbol{authority}, \boldsymbol{real\text{-}world\ interface}, \boldsymbol{rule\ space}) \quad \textbf{(1)}$$

For operational comparison, this framework can be developed into an **AI System Power Index (ASPI).** The index does not treat AI power as a directly observable quantity. Instead, it estimates the degree to which an AI system can produce real-world consequences within a specific institutional, operational, and rule environment.

Each dimension can be normalized to a **0–1** scale and combined through a weighted geometric mean:

$$\boldsymbol{ASPI = 100 \times M^{\alpha} \times D^{\beta} \times R^{\gamma} \times A^{\delta} \times I^{\varepsilon} \times S^{\zeta}} \quad \textbf{(2)}$$

where **M** represents model capability, **D** data quality, **R** resource access, A authority, I real-world interface, and S rule space. The parameters $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$, $\boldsymbol{\delta}$, $\boldsymbol{\varepsilon}$, and $\boldsymbol{\zeta}$ represent the weights assigned to each dimension, with the baseline condition that $\boldsymbol{\alpha + \beta + \gamma + \delta + \varepsilon + \zeta = 1}$.

The weights should not be fixed universally. A baseline model may use equal weights across all six dimensions. A policy assessment may use expert-derived weights. A sector-specific assessment may assign different weights depending on whether the system is deployed in public-facing services, enterprise operations, finance, health care, critical infrastructure, defense, or government administration.

The weighted geometric form is useful because it captures interaction effects. Strength in one dimension cannot fully compensate for near-zero capability in another. A highly capable model with limited data access, weak authority, or no operational interface may remain largely advisory. Conversely, a more specialized AI system with lower general capability may exert greater influence if it operates with high-quality proprietary data, institutional authority, resource access, and direct links to real-world systems.

Because the **geometric form** is sensitive to near-zero values, practical scoring requires clear thresholds for what counts as meaningful capability, data access, resource access, authority, interface connectivity, or rule-space permissiveness. Near-zero values should be used only when a system has no meaningful capability, access, authorization, operational interface, or permissive rule condition in the relevant dimension.

This distinction is central to the next stage of AI competition. The most consequential AI systems may not be the largest, most public-facing, or most widely used. They may be the systems most deeply embedded in economic, institutional, military, infrastructural, or regulatory environments. In this sense, AI power should be assessed not only by what a model can generate, but by what the surrounding system allows it to know, access, mobilize, do under authorization, and change.

The six dimensions can be summarized as follows:

Table 1. Six Dimensions of AI Power

Dimension	Core Question	Policy Relevance
Model Capability	What can the system process and perform?	Benchmarking and capability evaluation
Data Quality	What can it know?	Data governance and access control
Resource Access	What can it mobilize?	Compute, capital, and infrastructure oversight
Authority	Who allows it to act?	Authorization and accountability
Real-World Interface	What can it change?	API, workflow, and system control
Rule Space	Under what rules does it operate?	Legal scope, exemptions, and governance gaps

3. Components of AI Power

3.1 Model Capability

Model capability refers to the cognitive and technical performance of an AI system. It includes reasoning, planning, language processing, multimodal understanding, coding, prediction, simulation, adaptation, and task execution.

It is the cognitive foundation of AI power, but it is not equivalent to AI power itself. Without sufficient model capability, data, authority, and interfaces may not translate into effective performance. Yet a capable model without access, permission, or deployment channels remains largely informational rather than operational.

3.2 Data Quality

Data quality refers to the value, rarity, reliability, verification level, domain specificity, and operational relevance of the data available to an AI system.

Public data can provide breadth, but proprietary, restricted, classified, institutional, or experience-based data can provide strategic depth. In many domains, the most valuable data is not necessarily the largest dataset. It is the dataset that is trusted, timely, contextual, and actionable.

This suggests that future AI advantage may depend increasingly on access to specialized data environments, including medical records, industrial logs, financial flows, supply-chain data, defense intelligence, scientific datasets, legal archives, platform behavior, and real-time sensor streams.

3.3 Resource Access

Resource access refers to the assets an AI system can use, allocate, or influence. These may include compute, energy, capital, infrastructure, cloud platforms, sensors, logistics networks, financial systems, robotics, human labor, and physical devices.

Resource access determines whether AI remains a cognitive tool or becomes an operational actor. An AI system that only generates information has limited direct power. An AI system connected to procurement systems, trading platforms, factories, energy grids, logistics networks, or automated service platforms can produce material consequences.

The key question is therefore not only how intelligent an AI system is, but what it can mobilize.

3.4 Authority

Authority refers to the permission and mandate structure under which an AI system is allowed to act. It concerns who grants permission, who defines the system's operational role, and who authorizes its use in specific institutional or operational settings.

Authority may be organizational, contractual, administrative, legal, military, institutional, or platform-based. It determines whether a capability remains constrained, expanded, delegated, or operationalized.

The same model may be tightly constrained in a public-facing chatbot, expanded in an enterprise workflow, or authorized for use in government, infrastructure management, security, or emergency-response settings. Authority also determines accountability: once AI systems are embedded in institutions, their power depends not only on technical design, but also on who grants permission, who supervises execution, and who bears responsibility for outcomes.

3.5 Real-World Interface

A real-world interface refers to the channels through which an AI system connects to systems beyond the model environment. These interfaces may include software workflows, databases, APIs, markets, supply chains, infrastructure, physical devices, public services, legal processes, administrative platforms, or automated operational systems.

The interface is where AI moves from analysis to intervention. It is the channel through which AI can route goods, trigger alerts, allocate resources, modify schedules, approve claims, deny access, adjust prices, support prioritization decisions, or alter system states.

Without such interfaces, AI remains primarily advisory. With them, AI becomes capable of shaping outcomes.

3.6 Rule Space

Rule space refers to the legal, institutional, operational, and political environment that defines what an AI system is permitted, restricted, exempted, or enabled to do. It includes laws, regulations, institutional policies, platform rules, liability regimes, procurement rules, compliance requirements, emergency powers, national security exceptions, and gray-zone operating conditions.

Rule space is distinct from authority. Authority concerns who grants permission and operational mandate; rule space concerns the broader environment within which that permission is granted, constrained, expanded, or exercised.

Different rule spaces produce different AI deployment conditions. Public consumer AI is usually constrained by content policy, platform governance, liability concerns, and reputational risk. Enterprise AI may operate under contractual, compliance, and sectoral rules. Government and security-related AI may operate under public law, administrative procedure, classification regimes, emergency authorities, or special exemptions.

Rule space is therefore not merely an external constraint on AI power. It is a core variable that defines how AI power is permitted, limited, expanded, normalized, or released.

4. Strategic Implications

The next phase of AI competition will not be determined solely by who builds the most capable public-facing model. It will increasingly be shaped by who controls the broader conditions under which AI capability becomes consequential: high-quality data, compute and energy resources, institutional authority, operational infrastructure, deployment channels, and rule-making capacity.

This shifts the unit of analysis from the AI model to the AI power system. The most important actors may not simply be those with the best chatbot or the highest benchmark score, but those able to combine capable models with proprietary data, resource access, institutional permissions, platform control, legal authority, and real-world execution systems.

This shift has four strategic implications.

First, AI advantage may become less visible. Public rankings can show which models perform well in open evaluation settings, but they may not identify the systems with the greatest operational consequence. Some of the most powerful AI systems may operate inside firms, governments, militaries, financial platforms, industrial networks, or critical infrastructure.

Second, domain-specific AI may gain strategic importance. Systems trained or deployed in medicine, finance, logistics, energy, defense, manufacturing, public administration, or scientific research may exercise power through depth rather than scale. Their advantage may come from specialized data, workflow integration, institutional trust, and operational access rather than broad public visibility.

Third, institutional embedding may become a central axis of AI competition. The decisive question may be less “which model is best?” and more “which actor can place AI inside the most consequential systems?” AI systems embedded in decision processes, resource allocation mechanisms, infrastructure management, or security operations may have greater practical significance than more capable systems confined to public-facing interfaces.

Fourth, rule-making itself becomes a source of power. Actors able to define the legal, technical, and operational conditions for AI deployment can shape not only how AI is used, but what forms of AI power become possible. Standards, liability rules, procurement rules, data-access regimes, export controls, national security exemptions, and platform policies may all become instruments of AI power.

Taken together, these dynamics suggest that the strategic question is no longer only who has the strongest AI, but who controls the environment in which AI capability is connected to data, resources, authority, interfaces, and action.

5. Policy Implications

AI governance should move beyond the regulation of public interfaces alone. Content moderation, safety filters, transparency requirements, model evaluation, and public risk disclosure remain important. However, they do not fully address the deeper sources of AI power: data access, resource control, institutional authority, operational interfaces, and variation in rule space.

A system-centric governance framework should begin by asking a set of core questions:

- What data can the AI system access, learn from, or combine?
- What resources can it use, allocate, or influence?
- What decisions can it affect?
- What systems can it enter, modify, or control?
- What interfaces connect it to real-world operations?
- Who authorizes its actions?
- What legal, institutional, or operational rule space governs its deployment?
- What accountability mechanisms apply when it produces real-world consequences?

These questions should be translated into concrete governance practices.

First, regulators, public institutions, and deploying organizations should map AI system access and interfaces. High-consequence AI systems should be assessed not only by model capability, but also by their data access, API connections, execution permissions, resource calls, workflow integrations, and links to operational systems.

Second, AI systems should be classified by operational consequence, not only by model size or general capability. A system connected to financial markets, health care, public services, infrastructure, defense, or administrative decision-making may warrant heightened oversight even if its underlying model is not the most advanced public-facing model.

Third, high-consequence deployments should require clear authorization and accountability controls. Systems that can affect resource allocation, public services, infrastructure operations, security decisions, or institutional rights should include defined human authorization chains, logging, auditability, responsibility assignment, and mechanisms for appeal, suspension, or rollback.

The core governance question is therefore not only whether an AI system produces acceptable outputs. It is whether the system’s access, authority, interfaces, and intervention capacity are properly governed.

Such an approach would broaden AI governance from content safety to power governance: the governance of AI access, authority, interfaces, and intervention capacity. It would require closer attention to where AI systems are embedded, what they are connected to, who can authorize their use, and how responsibility is assigned when AI-enabled systems affect institutions, markets, infrastructure, or public services.

Limitations

This framework is conceptual and only partially operationalized. The proposed ASPI provides an index structure, but it does not prescribe universal indicators, weights, data sources, or measurement procedures across sectors, institutions, or national systems. A fully operational version of ASPI would require indicator-level definitions for each dimension, including data sources, scoring thresholds, normalization rules, and validation procedures.

The six components are analytically distinct but empirically interdependent. Data quality may depend on institutional authority; resource access may depend on rule space; and real-world interfaces may determine whether model capability remains advisory or becomes operational. In practice, these variables often reinforce or constrain one another.

The framework also does not assume that greater AI power is inherently beneficial or harmful. The same combination of capability, data, resources, authority, interfaces, and rules may support innovation, efficiency, market concentration, coercive control, or strategic instability depending on context. Further work is needed to develop measurable indicators, test alternative weighting schemes, and compare AI power systems across sectors, institutions, and countries.

Conclusion

AI power is not equivalent to model intelligence. It is a compound structure formed by model capability, data quality, resource access, authority, real-world interfaces, and rule space.

The future AI race will therefore not be only a race to build larger or more capable models. It will also be a race to control the conditions under which AI capability becomes consequential. Actors that combine capable models with high-quality data, resource channels, institutional authority, operational interfaces, and favorable rule environments may exercise influence that is not visible through public model rankings alone.

In simplified terms:

- Model capability determines what AI can process and perform.
- Data determines what AI can know.
- Resources determine what AI can mobilize.
- Authority determines what AI can do.
- Interfaces determine what AI can change.
- Rules determine what AI is allowed to become.

Understanding AI power requires analyzing these dimensions together. Only then can policymakers, firms, and researchers assess not only how capable an AI system is, but how much real-world influence it may exercise.

References

AI Index Steering Committee, Stanford Institute for Human-Centered Artificial Intelligence. (2026). *The 2026 AI Index report*. Stanford University. https://hai.stanford.edu/ai-index/2026-ai-index-report

Kim, R. M., Kuehnert, B., Lazar, S., Singh, R., & Heidari, H. (2025). The AI Power Disparity Index: Toward a compound measure of AI actors' power to shape the AI ecosystem. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 8*(2), 1453–1464. https://doi.org/10.1609/aies.v8i2.36645

Oxford Insights. (2025). *Government AI Readiness Index 2025*. https://oxfordinsights.com/ai-readiness/government-ai-readiness-index-2025/

Tortoise Media. (2024). *The Global AI Index*. https://www.tortoisemedia.com/data/global-ai