

GEOPOLITICS OF AI

Technology as an Instrument of Global Power

Rudy C Tarumingkeng

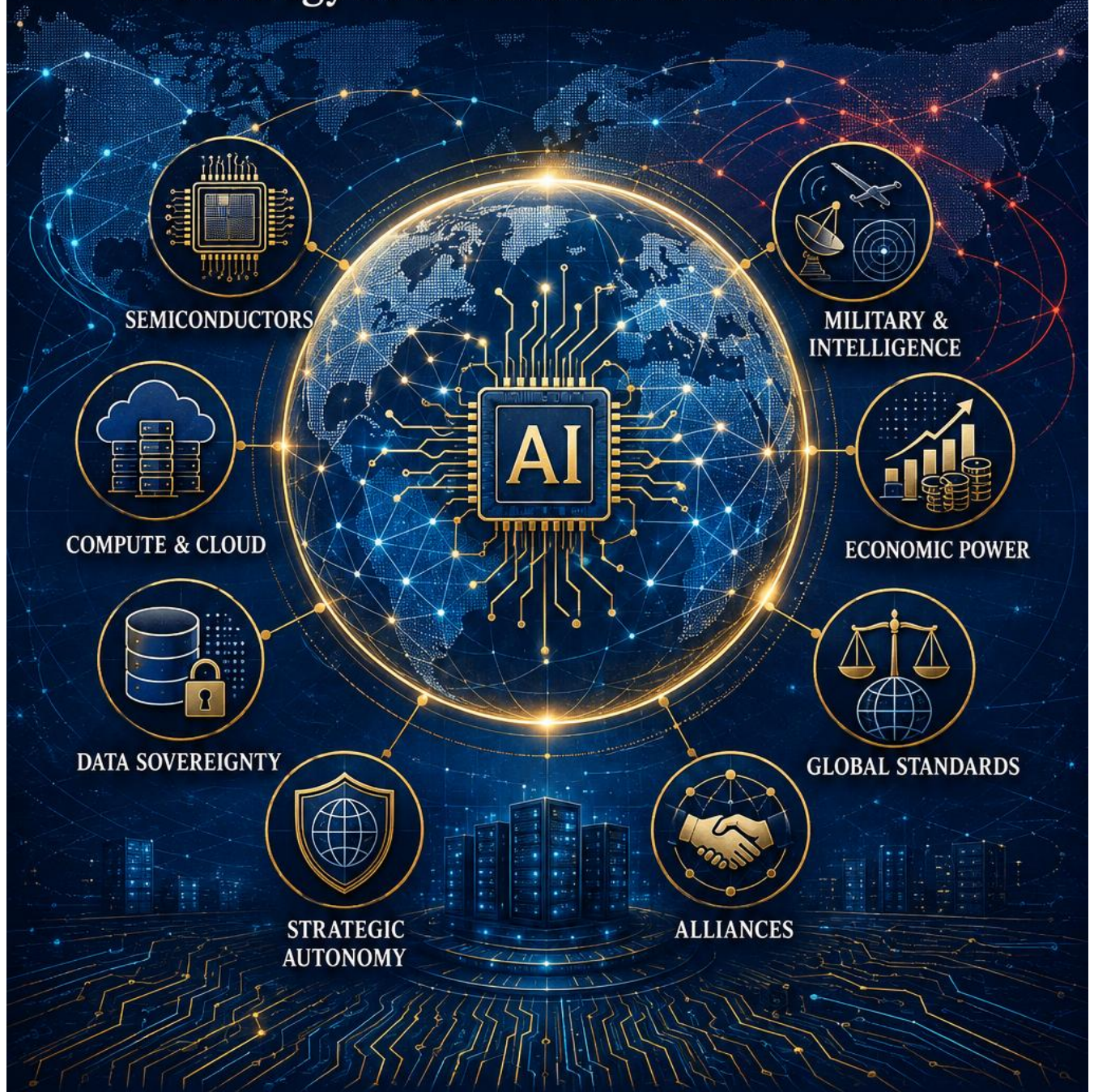
www.rudyclt.com/cv.pdf

RudyCT Academic Series 2026

Bogor, Indonesia • July 2026

GEOPOLITICS OF AI

Technology as an Instrument of Global Power



By: Rudy C Tarumingkeng

RudyCT Academic Series 2026

Abstract

Artificial intelligence has become an instrument of global power because frontier capability depends on strategic resources: advanced semiconductors, compute infrastructure, cloud platforms, energy, data, talent, capital, and standards. This article examines the geopolitics of AI as a socio-technical struggle involving states, firms, alliances, and international institutions. It analyzes the U.S.–China rivalry, the European Union’s regulatory power, East Asian semiconductor chokepoints, digital middle powers, export controls, military applications, information warfare, data sovereignty, corporate power, and the AI divide affecting the Global South. Particular attention is given to Indonesia and ASEAN. The central argument is that AI leadership cannot be measured only by model performance; it also depends on resilience, legitimacy, governance, alliances, and the capacity to distribute benefits. A stable AI order requires strategic competition bounded by responsibility, meaningful human control, plural participation, and continued cooperation on shared risks.

Keywords: artificial intelligence; geopolitics; global power; semiconductors; compute sovereignty; U.S.–China rivalry; export controls; AI governance; strategic autonomy; Indonesia; ASEAN

Executive Synthesis

- AI power rests on material infrastructure as well as algorithms.
- Semiconductor and cloud chokepoints convert economic interdependence into geopolitical leverage.
- States compete through subsidies, export controls, standards, regulation, alliances, and talent policy.
- Private technology firms exercise quasi-sovereign power but remain dependent on states and global supply chains.
- Indonesia and ASEAN need principled strategic autonomy built on capacity, regional cooperation, and open standards.

Introduction: AI Enters the Arena of World Power

Introduction: AI Enters the Arena of World Power is best understood through the transformation of artificial intelligence from a commercial technology into a strategic asset. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include economic competitiveness, military capability, intelligence, diplomacy, and ideological influence. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve the fusion of private innovation with state power. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks a new geography organized around compute, data, talent, energy, and alliances. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

1. Conceptualizing the Geopolitics of AI

1. Conceptualizing the Geopolitics of AI is best understood through the study of how territory, infrastructure, institutions, and technological capability shape international power. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial

concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include material resources and narratives of legitimacy. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve the assumption that software is placeless. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks a socio-technical field in which code depends on globally distributed physical systems. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

2. AI as a General-Purpose and Dual-Use Technology

2. AI as a General-Purpose and Dual-Use Technology is best understood through AI applications that transform multiple sectors and can serve both civilian and military purposes. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include productivity, science, logistics, security, and command. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains;

regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve the difficulty of separating beneficial diffusion from strategic risk. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks governance that distinguishes capabilities, users, contexts, and consequences. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

3. The Compute–Chip–Cloud Power Triangle

3. The Compute–Chip–Cloud Power Triangle is best understood through advanced semiconductors, high-performance computing, data centers, and cloud platforms. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include control over the means of training and deploying frontier models. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve concentration, chokepoints, export restrictions, and extraterritorial leverage. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid

collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks compute sovereignty balanced with international interdependence. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

4. Semiconductor Chokepoints and Supply-Chain Geography

4. Semiconductor Chokepoints and Supply-Chain Geography is best understood through the geographically concentrated production of design software, lithography, fabrication, packaging, memory, and equipment. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include industrial specialization and alliance networks. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve earthquakes, conflict, coercion, sanctions, and single-source dependence. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks diversification, stockpiles, trusted supply chains, and strategic redundancy. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

5. The United States: Platform, Capital, and Alliance Power

5. The United States: Platform, Capital, and Alliance Power is best understood through a technology ecosystem combining frontier firms, venture capital, universities, cloud infrastructure, and security alliances. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include innovation scale and control over key technologies. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve commercial concentration and the securitization of global markets. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks maintaining leadership without fragmenting science and trade. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States

that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

6. China: State Capacity and Technological Self-Reliance

6. China: State Capacity and Technological Self-Reliance is best understood through a national strategy linking industrial policy, data-rich platforms, research, standards, and civil–military objectives. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include scale, coordination, manufacturing, and long-term investment. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve external controls, internal inefficiencies, and trust concerns. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks indigenous capability and alternative international technology networks. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers,

customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

7. The European Union: Regulatory and Market Power

7. The European Union: Regulatory and Market Power is best understood through the use of a large market and legal standards to shape global AI practices. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include rights-based regulation, safety, competition, and the Brussels effect. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve implementation complexity and a frontier-capability gap. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks normative influence combined with strategic investment. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing

countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

8. Taiwan, South Korea, Japan, and the Strategic Asian Core

8. Taiwan, South Korea, Japan, and the Strategic Asian Core is best understood through the centrality of East Asian semiconductor fabrication, memory, materials, equipment, and advanced manufacturing. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include technological specialization and alliance value. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve exposure to regional conflict, coercion, and industrial relocation. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks resilient interdependence and distributed capacity. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

9. India and the Rise of Digital Middle Powers

9. India and the Rise of Digital Middle Powers is best understood through the use of digital public infrastructure, a vast talent base, diplomacy, and market scale. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include strategic autonomy and development-oriented AI. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve compute constraints, linguistic diversity, and uneven access. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks coalition building outside rigid great-power blocs. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

10. The Gulf States and Compute Diplomacy

10. The Gulf States and Compute Diplomacy is best understood through sovereign wealth, energy resources, data-center investment, and partnerships with rival technology ecosystems. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis

therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include rapid infrastructure building and diplomatic leverage. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve dependency on imported chips, expertise, and security guarantees. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks new hubs linking capital, energy, and global model access. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

11. Russia and AI under Strategic Constraint

11. Russia and AI under Strategic Constraint is best understood through the integration of AI with military, cyber, information, and surveillance capabilities. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include state security applications and asymmetric power. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation

can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve sanctions, limited access to advanced hardware, and talent loss. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks selective innovation under geopolitical isolation. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

12. Data Sovereignty and the Politics of Digital Territory

12. Data Sovereignty and the Politics of Digital Territory is best understood through claims that data generated by citizens, firms, and public institutions should remain under legitimate national or regional control. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include privacy, security, industrial development, and regulatory autonomy. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve localization costs, surveillance, and fragmented markets. Policies intended to protect security may create unintended consequences: firms redesign products,

supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks trusted cross-border data arrangements with enforceable safeguards. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

13. Models, Languages, and Cultural Power

13. Models, Languages, and Cultural Power is best understood through foundation models that encode language, knowledge, values, and patterns of representation. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include agenda setting, epistemic influence, education, media, and cultural visibility. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve linguistic marginalization, bias, dependency, and narrative manipulation. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks plural AI ecosystems that support local languages and knowledge. It distinguishes genuine security threats from commercial protectionism, defines

measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

14. Standards as Instruments of Power

14. Standards as Instruments of Power is best understood through technical and governance standards that determine interoperability, safety, benchmarks, documentation, and market access. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include coordination, trust, and first-mover advantage. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve standards capture and the export of political assumptions. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks open, multistakeholder, and globally legitimate rulemaking. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

15. Export Controls and Technological Containment

15. Export Controls and Technological Containment is best understood through restrictions on advanced chips, manufacturing equipment, software, model weights, and technical services. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include delaying military-relevant capability and protecting strategic advantage. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve evasion, substitution, market fragmentation, and accelerated self-reliance. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks targeted, adaptive, coalition-based controls with clear objectives. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid

authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

16. AI, Military Transformation, and Deterrence

16. AI, Military Transformation, and Deterrence is best understood through autonomy, intelligence analysis, targeting support, logistics, cyber operations, simulation, and decision support. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include speed, precision, situational awareness, and force multiplication. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve escalation, accidental conflict, accountability gaps, and machine-speed instability. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks meaningful human control and crisis-stability safeguards. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may

strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

17. Information Warfare and Cognitive Security

17. Information Warfare and Cognitive Security is best understood through the use of generative systems for persuasion, synthetic media, microtargeting, translation, and influence operations. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include strategic communication and scalable content production. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve disinformation, impersonation, erosion of trust, and epistemic fragmentation. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks provenance, media literacy, platform accountability, and resilient institutions. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

18. Intelligence, Surveillance, and Authoritarian Power

18. Intelligence, Surveillance, and Authoritarian Power is best understood through AI-enabled pattern detection, biometrics, predictive policing, social monitoring, and border control. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include security and administrative reach. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve repression, discriminatory profiling, chilling effects, and technology export. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks rights-preserving oversight and strict limits on high-risk uses. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

19. AI Diplomacy and Global Governance

19. AI Diplomacy and Global Governance is best understood through negotiation over principles, safety, access, standards, incident reporting, and capacity building. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial

concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include cooperation on transboundary risks and shared benefits. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve forum shopping, rival blocs, symbolic declarations, and enforcement gaps. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks layered governance connecting universal principles with technical mechanisms. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

20. The Global South and the AI Power Divide

20. The Global South and the AI Power Divide is best understood through unequal access to compute, capital, datasets, research networks, and bargaining power. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include development applications and new forms of technological leapfrogging. These sources of power interact rather than operate separately. Technical

leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve digital dependency, extractive data relations, and imported governance. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks capability partnerships, regional infrastructure, and fair access. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

21. Corporate Sovereignty and Private Power

21. Corporate Sovereignty and Private Power is best understood through frontier laboratories and cloud platforms controlling infrastructure, models, talent, safety knowledge, and deployment channels. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include innovation speed and global service capacity. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve private rulemaking without democratic legitimacy and too-big-to-exit dependencies. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks public accountability, competition, interoperability, and procurement leverage. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

22. Energy, Water, Minerals, and the Physical Limits of AI

22. Energy, Water, Minerals, and the Physical Limits of AI is best understood through the material resources required for data centers, chips, cooling, grids, and device supply chains. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include energy diplomacy, industrial location, and infrastructure development. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve environmental externalities, local conflict, and resource competition. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by

effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks transparent, efficient, low-carbon, and locally legitimate compute expansion. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

23. Scientific Openness versus National Security

23. Scientific Openness versus National Security is best understood through international research exchange, open publication, talent mobility, and reproducibility under security pressure. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include scientific progress and collective problem solving. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve knowledge leakage, discriminatory restrictions, and weakened collaboration. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks risk-based research security that preserves openness where possible. It distinguishes genuine security threats from commercial protectionism, defines

measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

24. Indonesia and ASEAN: Strategic Autonomy in an AI World

24. Indonesia and ASEAN: Strategic Autonomy in an AI World is best understood through regional market scale, critical minerals, data-center growth, digital entrepreneurship, and non-aligned diplomatic traditions. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include human capital, language technology, regional standards, and public-interest infrastructure. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve dependency on foreign clouds and models, talent gaps, and regulatory fragmentation. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks ASEAN cooperation and Indonesian capacity for principled multi-alignment. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy

is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

25. Scenarios for the Emerging AI Order

25. Scenarios for the Emerging AI Order is best understood through alternative futures of open interdependence, managed rivalry, hardened blocs, or corporate feudalism. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include foresight as a tool for robust strategy. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve linear prediction in a rapidly changing system. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks policies that preserve options, resilience, and channels for cooperation. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid

authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

Conclusion: Power, Responsibility, and Human Agency

Conclusion: Power, Responsibility, and Human Agency is best understood through the recognition that AI power is produced through choices about infrastructure, institutions, alliances, and values. Artificial intelligence appears intangible, yet its production and use depend on physical territory, industrial concentration, energy, finance, skilled labor, law, and political authority. Geopolitical analysis therefore asks not only who has the most capable models, but who controls the infrastructures, standards, supply routes, knowledge networks, and alliances that make capability possible.

The strategic assets include security, prosperity, dignity, and global stability. These sources of power interact rather than operate separately. Technical leadership can attract capital and talent; market scale can shape standards; military alliances can secure supply chains; regulation can influence firms beyond national borders. Power lies in the ability to combine assets, withstand disruption, and set the terms on which others participate.

The principal risks involve technological determinism and winner-takes-all fatalism. Policies intended to protect security may create unintended consequences: firms redesign products, supply chains reroute through third countries, researchers avoid collaboration, and targeted states accelerate substitution. Geopolitical tools must therefore be evaluated by effectiveness, proportionality, alliance cohesion, economic cost, and effects on long-term innovation.

A strategically responsible approach seeks a plural and governable AI order in which human responsibility remains central. It distinguishes genuine security threats from commercial protectionism, defines measurable objectives, consults allies and affected countries, and preserves channels for scientific and diplomatic cooperation. It also recognizes that legitimacy is a form of power. States that offer credible rules, public goods, and respectful partnerships may shape the global order more durably than those relying only on coercion.

Geopolitics operates through firms as well as governments. Semiconductor designers, foundries, cloud providers, frontier laboratories, telecom operators, and platform companies make choices with national-security consequences. Yet these firms are transnational: their investors, workers, customers, facilities, and suppliers cross jurisdictions. Public policy must manage this hybrid authority without assuming that corporate incentives automatically coincide with national or global interests.

The distributive dimension is equally important. Restrictions, subsidies, and infrastructure investments create winners and losers within countries and across regions. A policy may strengthen a national champion while raising costs for universities, small firms, or developing

countries. Responsible statecraft makes these effects visible and builds adjustment, capacity sharing, and remedy into strategy. Otherwise, AI rivalry can deepen inequality and weaken the international cooperation needed for safety, climate, health, and development.

Geopolitical Capability Matrix

Domain	Key resources	Strategic effect
Compute	Data centers, accelerators, cloud access	Training and deployment capacity
Semiconductors	Design, equipment, fabrication, memory, packaging	Chokepoint and industrial leverage
Data	High-quality, lawful, representative datasets	Model relevance and intelligence
Talent	Researchers, engineers, operators, policy expertise	Innovation and absorptive capacity
Energy	Reliable low-carbon electricity and cooling	Cost, scale, and strategic location
Capital	Public funding, venture finance, procurement	Speed and ecosystem depth
Standards	Technical rules, benchmarks, regulation	Market access and normative influence
Alliances	Trusted networks and diplomatic partnerships	Resilience, legitimacy, and coordinated action

Strategic Recommendations for Indonesia and ASEAN

1. Develop shared regional compute facilities for research, public-interest AI, and SMEs.
2. Invest in advanced digital skills, semiconductor talent, safety evaluation, and public-sector expertise.
3. Support Indonesian and ASEAN languages through lawful, representative, community-informed datasets.
4. Adopt interoperable standards and procurement rules that reduce vendor lock-in.
5. Strengthen cybersecurity, data governance, and critical-infrastructure resilience.
6. Use critical-mineral policy to build higher-value capabilities without creating new ecological or social harm.
7. Coordinate ASEAN positions in global AI governance forums while preserving national diversity.
8. Negotiate technology partnerships that include knowledge transfer, local research, and credible security guarantees.
9. Distinguish targeted national-security controls from broad protectionism.

10. Build independent model evaluation and incident-reporting capacity.
11. Protect academic exchange while implementing proportionate research-security safeguards.
12. Develop transparent rules for military, surveillance, biometric, and other high-risk AI uses.
13. Promote competition and portability in cloud and platform markets.
14. Align data-center expansion with renewable energy, water constraints, and local benefit.
15. Practice principled multi-alignment: cooperate widely without surrendering policy autonomy.

Extended Academic Synthesis

The geopolitics of AI reveals a paradox. Digital systems can cross borders instantly, but frontier capability depends on highly localized and capital-intensive infrastructure. Advanced lithography equipment, leading-edge fabrication, specialized memory, high-speed networking, and hyperscale clouds are concentrated in a small number of firms and jurisdictions. This concentration gives states leverage, but also creates common vulnerability. No major power is completely autonomous.

Interdependence therefore becomes both a source of efficiency and a potential weapon. Export controls, investment screening, entity restrictions, procurement bans, and sanctions exploit network position. Yet coercion can motivate substitution, divide alliances, and reduce the controlling country's market share or information. The strategic question is not whether interdependence exists, but how it is governed and whether reliance remains politically tolerable.

AI competition also differs from earlier arms races because private firms own much of the relevant infrastructure and expertise. Governments depend on companies for models, chips, cloud services, and threat information. Companies depend on governments for research, energy, education, intellectual property, security, and market access. This mutual dependence requires new accountability arrangements that neither nationalize innovation nor allow private actors to determine public risk alone.

Normative power matters alongside material power. Countries and regions that define credible rules can shape product design and global expectations. However, rules without capability may produce dependency, while capability without legitimacy may provoke resistance. Durable influence combines innovation, market scale, reliable alliances, rights-respecting governance, and the provision of global public goods such as safety research and capacity building.

The Global South is not a passive arena. States can bargain, form regional coalitions, develop language and sectoral applications, and demand fairer terms for data and infrastructure. Nevertheless, weak compute access and dependence on foreign platforms can narrow choices. Development cooperation should move beyond user training toward research capability, shared compute, regulatory expertise, open standards, and institutions able to negotiate with multinational firms.

Military AI creates particular urgency. Speed can improve defense but compress decision time and increase automation bias. Systems trained in peacetime conditions may fail under deception or adversarial attack. Meaningful human control requires more than formal authorization; it requires sufficient information, time, competence, and authority. Crisis hotlines, testing norms, and constraints on high-risk autonomy may support strategic stability even among rivals.

Information warfare threatens the epistemic foundations of diplomacy and democracy. Synthetic media can impersonate leaders, fabricate events, and saturate networks with uncertainty. The problem is not only believing a specific falsehood; it is losing confidence that evidence can be known. Technical provenance helps, but resilient journalism, trusted institutions, civic education, and rapid authenticated communication are equally important.

Environmental constraints may reshape the map of AI power. Data centers seek reliable electricity, cooling, water, land, connectivity, and political stability. Regions with low-carbon energy may gain advantage, while local communities may resist projects that compete for scarce resources. Compute policy must therefore integrate energy strategy, grid planning, environmental justice, and transparent benefit sharing.

For Indonesia, strategic autonomy should not be confused with isolation. The country benefits from diverse partnerships, open research, foreign investment, and regional trade. Autonomy means retaining the capability to evaluate offers, protect legitimate interests, switch providers, develop local talent, and contribute to rules. ASEAN can multiply bargaining power by coordinating standards, infrastructure, and diplomatic positions.

The future AI order remains open. Rivalry may harden into blocs, or managed interdependence may persist. Corporate platforms may gain quasi-sovereign authority, or public institutions may restore accountability. Foresight encourages governments and firms to preserve options: diversify dependencies, maintain dialogue, invest in local capability, and create institutions able to adapt. Power will belong not only to those who build the most capable systems, but to those who govern them wisely and earn cooperation.

Glossary

AI diplomacy: Use of diplomatic relations and international forums to shape AI cooperation, access, rules, and capacity.

AI sovereignty: Capacity of a state or region to make legitimate choices about AI infrastructure, data, models, and governance.

Brussels effect: Global influence created when firms adopt EU rules to retain access to its large market.

Chokepoint: A concentrated technology, supplier, route, or capability whose control creates strategic leverage.

Compute: Computational resources used to train, evaluate, and operate AI systems.

Compute divide: Unequal access to affordable, suitable, and governable computing resources.

Corporate sovereignty: Quasi-governing power exercised by firms controlling essential digital infrastructure or platforms.

Critical technology: Technology considered essential to security, economic resilience, or strategic advantage.

Data localization: Requirement that specified data be stored or processed within a jurisdiction.

Data sovereignty: Authority to govern data according to legitimate national, regional, or community rules.

Dual-use technology: Technology with both civilian and military or security applications.

Export control: Legal restriction on transfer of specified goods, software, technology, or services to foreign destinations or users.

Foundation model: A large general-purpose model adaptable to many downstream applications.

Geoeconomics: Use of economic instruments and relationships to pursue geopolitical objectives.

Geopolitics of AI: Study of how AI capabilities, infrastructures, rules, and dependencies shape international power.

Meaningful human control: Human understanding, authority, and responsibility sufficient to govern consequential system action.

Model weights: Numerical parameters learned during model training that encode operational capability.

Regulatory power: Ability to shape behavior and markets through rules, standards, and enforcement.

Strategic autonomy: Capacity to make and implement important choices without unacceptable external dependence.

Techno-nationalism: Policy orientation linking technological capability to national identity, security, and power.

References

- Allen, G. C. (2022). Choking off China's access to the future of AI. Center for Strategic and International Studies.
- Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press. <https://doi.org/10.1093/oso/9780190088583.001.0001>
- Bremmer, I. (2021). The technopolar moment. *Foreign Affairs*, 100(6), 112–128.
- Cave, S., & Dihal, K. (2020). The whiteness of AI. *Philosophy & Technology*, 33, 685–703. <https://doi.org/10.1007/s13347-020-00415-6>
- Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics. *Contemporary Security Policy*, 41(1), 7–32. <https://doi.org/10.1080/13523260.2019.1678855>
- European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.
- Farrell, H., & Newman, A. L. (2019). Weaponized interdependence. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351

- Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A*, 376, 20180081. <https://doi.org/10.1098/rsta.2018.0081>
- Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review*, 1(3), 37–57. <https://doi.org/10.26153/tsw/884>
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
- Kello, L. (2013). The meaning of the cyber revolution. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138
- Khan, S. M., Mann, A., & Peterson, D. (2021). The semiconductor supply chain: Assessing national competitiveness. Center for Security and Emerging Technology. <https://doi.org/10.51593/20190016>
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>
- Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Scribner.
- Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.
- OECD. (2023). A blueprint for building national compute capacity for artificial intelligence. OECD Digital Economy Papers, No. 350. <https://doi.org/10.1787/876367e3-en>
- Payne, K. (2018). Artificial intelligence: A revolution in strategic affairs? *Survival*, 60(5), 7–32. <https://doi.org/10.1080/00396338.2018.1518374>
- Roberts, H., Cows, J., Morley, J., et al. (2021). The Chinese approach to artificial intelligence. *AI & Society*, 36, 59–77. <https://doi.org/10.1007/s00146-020-00992-2>
- Schmidt, E., Work, R., Catz, S., et al. (2021). Final report. National Security Commission on Artificial Intelligence.
- Sevilla, J., Heim, L., Ho, A., Besiroglu, T., Hobbhahn, M., & Villalobos, P. (2022). Compute trends across three eras of machine learning. 2022 International Joint Conference on Neural Networks. <https://doi.org/10.1109/IJCNN55064.2022.9891914>
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752. <https://doi.org/10.1126/science.aat5991>
- U.S. Department of Commerce, Bureau of Industry and Security. (2022). Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the People's Republic of China.
- Walters, R. (2022). *AI and the future of global affairs*. Edward Elgar. <https://doi.org/10.4337/9781800882607>
- Zwetsloot, R. (2019). China's approach to tech talent competition. Center for Security and Emerging Technology. <https://doi.org/10.51593/20190005>