OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 17, Nº. 2
November 2026-April 2027

JANUS.NET
e-journal of International Relations

FROM DETERRENCE TO DEPENDENCE: THE STRATEGIC LOGIC OF TECHNOLOGICAL ALLIANCES IN THE AI ERA

ALP CENK ARSLAN
alpcenkarslan@gmail.com
Turkish National Police Academy (Türkiye). https://orcid.org/0000-0002-5526-2089

Abstract

The architecture of global security is undergoing a structural transformation as artificial intelligence (AI) becomes the foundation of power in international relations. Traditional security alliances, once organized around deterrence and collective defense, are increasingly defined by technological interdependence. This article argues that in the AI era, deterrence has evolved into dependence, a condition in which states' strategic stability relies not only on military cooperation but also on shared technological infrastructures, standards, and supply chains. Through a comparative analysis of the United States, the European Union, and China, the study examines how techno-alliances such as the U.S.-led "Chip 4 Alliance," the EU's Digital Sovereignty agenda, and China's Digital Silk Road reconfigure global power hierarchies. The analysis shows that technology has become both the medium and the object of strategic competition, producing asymmetric dependencies that blur the distinction between allies and rivals. Drawing from strategic studies and techno-political theory, the paper conceptualizes technological dependence as a new form of structural power, where control over data, compute, and infrastructure determines geopolitical leverage. The findings suggest that managing interdependence, rather than achieving dominance, will define strategic success in the coming decade. The study concludes by outlining implications for global governance, emphasizing adaptive security strategies that reflect the political economy of digital infrastructure and the emerging logic of techno-political alignment.

Keywords

Security architecture; technological interdependence; AI; Technopolitical Theory.

Resumo

A arquitetura da segurança global está a passar por uma transformação estrutural, à medida que a inteligência artificial (IA) se torna a base do poder nas relações internacionais. As alianças de segurança tradicionais, outrora organizadas em torno da dissuasão e da defesa coletiva, são cada vez mais definidas pela interdependência tecnológica. Este artigo defende que, na era da IA, a dissuasão evoluiu para a dependência, uma condição em que a estabilidade estratégica dos Estados depende não só da cooperação militar, mas também de infraestruturas tecnológicas, normas e cadeias de abastecimento partilhadas. Através de uma análise comparativa dos Estados Unidos, da União Europeia e da China, o estudo examina como as alianças tecnológicas, tais como a «Aliança Chip 4» liderada pelos EUA, a agenda de Soberania Digital da UE e a Rota da Seda Digital da China, reconfiguram as hierarquias de poder globais. A análise mostra que a tecnologia se tornou tanto o meio como o objeto da competição estratégica, produzindo dependências assimétricas que esbatem a distinção entre aliados e rivais. Com base em estudos estratégicos e na teoria tecnopolítica, o artigo conceptualiza a dependência tecnológica como uma nova forma de poder estrutural, em que o controlo sobre os dados, a capacidade computacional e as infraestruturas determina a influência geopolítica. As conclusões sugerem que a gestão da interdependência, em vez da

conquista do domínio, definirá o sucesso estratégico na próxima década. O estudo conclui delineando implicações para a governação global, enfatizando estratégias de segurança adaptativas que reflitam a economia política das infraestruturas digitais e a lógica emergente do alinhamento tecnopolítico.

Palavras-chave

Arquitetura de segurança; interdependência tecnológica; IA; Teoria Tecnopolítica.

How to cite this article
Arslan, Alp Cenk (2026). From Deterrence to Dependence: The Strategıc Logıc of Technologıcal Allıances in the AI Era. *Janus.net, e-journal of international relations*. VOL. 17, Nº. 2, November 2026-April 2027, pp. 72-89. DOI https://doi.org/10.26619/1647-7251.17.2.4

Article submitted on 6 November 2025 and accepted on 18 July 2026.

FROM DETERRENCE TO DEPENDENCE: THE STRATEGIC LOGIC OF TECHNOLOGICAL ALLIANCES IN THE AI ERA

ALP CENK ARSLAN

Introduction: The New Silicon Curtain

The contemporary geopolitical landscape is increasingly defined by an intense and systemic rivalry between the United States and China. This competition, however, does not conform to the familiar contours of past great power struggles. It signals the dawn of a new era characterized by a "Silicon Curtain", a global division based not on ideology or military blocs in the traditional sense, but on bifurcated technological ecosystems with semiconductors and artificial intelligence at their core. This transformation represents a foundational shift in global power dynamics, where control over advanced silicon is increasingly equated with national security and AI supremacy. The long-standing model of a hyper-globalized, efficiency-optimized supply chain is giving way to a more fragmented, security-centric regionalization, fundamentally altering the terrain of international conflict and cooperation (TokenRing AI, 2025).

This new reality poses a profound challenge to the established theoretical frameworks of international relations. Classic deterrence theory, the intellectual bedrock of strategic thought for over half a century, appears increasingly insufficient to explain or navigate this emerging dynamic. Forged in the crucible of the Cold War and oriented around the threat of nuclear annihilation, deterrence logic relies on assumptions of rational actors, clear signaling, credible threats of retaliation, and a shared understanding of catastrophic costs, conditions that are systematically eroded in the age of AI (Wong et al., 2020). The core argument of this manuscript is that strategic power is no longer exercised primarily through the threat of conventional or nuclear force, but through the cultivation, manipulation, and weaponization of technological dependencies.

To substantiate this claim, this manuscript undertakes a three-part intellectual journey. Initial part of the study provides a critical examination of classic deterrence theory, demonstrating its theoretical and practical failures when confronted with the unique characteristics of AI-driven conflict. It argues that the speed, opacity, and preemptive nature of AI do not merely complicate deterrence but fundamentally invert its logic. The remainder of the study constructs a new theoretical framework to explain the emerging strategic paradigm. It maps the global AI and semiconductor supply chains as the new strategic terrain and introduces the concept of "technological dependence" as a form of structural power. This framework posits that control over critical network nodes, or chokepoints, in these supply chains allows states to shape the behavior of others by setting the very terms of their participation in the modern global economy. Finally, the

final part applies this framework to the contemporary strategies of the United States, the European Union, and China. It analyzes how each of these major powers is attempting to navigate this new landscape by either architecting chokepoints, pursuing regulatory and technological sovereignty, or building a parallel, self-reliant ecosystem. The manuscript concludes by reframing the security dilemma for the 21st century, moving from the logic of Mutually Assured Destruction to a new, more complex reality of Mutually Assured Disruption.

The Erosion of Classic Strategic Logics

The Brittle Pillars of Deterrence in the Algorithmic Age

The strategic architecture of the post-World War II international system was built upon the intellectual foundation of deterrence. This theory, while evolving over time, provided a coherent logic for managing great power competition and avoiding catastrophic conflict. However, the integration of artificial intelligence and autonomous systems into the sinews of national security is rendering this foundational logic obsolete. The speed, ambiguity, and offensive potential inherent in AI technologies challenge the core assumptions of deterrence, creating a strategic environment for which the classic models are dangerously ill-suited.

At its core, deterrence is the practice of discouraging an adversary from taking an unwelcome action through the threat of force. As Thomas Schelling defined it, deterrence aims "to prevent from action by fear of consequences". This strategic effect is achieved through two primary mechanisms. The first, deterrence by punishment, involves persuading an opponent that the costs of an action will be unacceptably high due to a credible threat of retaliation. The second, deterrence by denial, seeks to convince an adversary that its aggressive action is unlikely to succeed, thereby denying it the anticipated benefits of the attack (Rühle, 2015). Most classic studies suggest that denial strategies, such as placing significant military forces in the path of a potential aggressor, are inherently more reliable than punishment strategies, which may be undermined by doubts about the deterrer's resolve to follow through on its threats (Mazarr, 2018).

The efficacy of deterrence rests on a set of critical assumptions, most notably the rationality of the actors involved. Rational deterrence theory posits that states behave as unitary, rational actors engaged in a cost-benefit calculus. In this model, both a "Challenger" seeking to alter the status quo and a "Defender" seeking to preserve it recognize that open conflict is the worst possible outcome for all parties. For deterrence to succeed, the Defender must persuade the Challenger of three things: that it possesses an effective military capability; that this capability can impose unacceptable costs; and that the threat to use it is credible. This triad of capability, credibility, and clear communication forms the essential components of a successful deterrence strategy (Quackenbush, 2011).

The concept of credibility is central, representing an actor's perceived willingness to execute its deterrent threat even when doing so is costly (Moreira, 2019). During the Cold War, for example, the United States sought to enhance the credibility of its nuclear deterrent through "irrevocable commitments", such as stationing troops in Europe, which acted as a tripwire that would make a retaliatory response nearly automatic

(Quackenbush, 2011). This logic was applied across different contexts, giving rise to important distinctions within the theory. General deterrence refers to the ongoing, persistent efforts to prevent conflict in non-crisis situations, whereas immediate deterrence involves urgent attempts to prevent a specific, imminent attack. Similarly, direct deterrence concerns the protection of a state's own territory, while extended deterrence involves the protection of allies, a cornerstone of alliances like NATO. It was this complex but coherent framework that guided strategic planning and, many argue, maintained a fragile peace between the superpowers for decades.

The introduction of artificial intelligence into military and strategic affairs fundamentally disrupts the logic that underpinned classic deterrence. AI does not merely add a new weapon to the arsenal; it alters the nature of conflict and decision-making in ways that undermine the theory's foundational pillars.

First, the core assumption of a predictable, rational actor breaks down when confronted with a complex human-machine assemblage. Classic deterrence is a psychological theory at its heart, involving humans attempting to dissuade other humans (Wong et al., 2020). The introduction of AI means that decision-making processes are "no longer fully under the control of humans" (AUSA, 2020). AI systems, particularly those based on advanced machine learning, can exhibit emergent behaviors and follow decision pathways that are opaque even to their human creators, challenging the very notion of predictable, rational action. This opacity is compounded by the problem of speed. AI and autonomous systems operate at machine speeds, compressing or eliminating the time for human deliberation, which is a critical component of rational strategic assessment. Wargames simulating conflicts involving autonomous systems have demonstrated that this speed can lead directly to inadvertent escalation, as automated responses spiral out of control faster than humans can intervene. This speed mismatch creates a profound crisis instability, where the carefully calibrated signaling and de-escalation tactics of classic deterrence become impossible to execute (Wong et al., 2020). Wong et al. (2020) therefore caution that machine-speed decision cycles can encourage early use and increase the risks of inadvertent escalation and crisis instability, making calibrated signaling and timely de-escalation more difficult.

Second, AI exacerbates the attribution problem to a degree that cripples deterrence by punishment. AI-enabled capabilities are ideal for conducting gray-zone, hybrid, and cyber operations that are deliberately designed to be ambiguous and difficult to trace to a specific state actor. These operations often involve multiple proxy actors and span hazy domains like information operations and economic influence, making a clear connection to a state sponsor difficult to establish (Lynch & Morrison, 2023). Without clear and timely attribution, the threat of targeted retaliation, the very essence of deterrence by punishment, loses its meaning. As experts succinctly puts it, "you cannot deter unless you can punish and you cannot effectively punish unless you have attribution" (Lynch & Morrison, 2023). A threat of retaliation that cannot be directed at a specific aggressor is an empty threat.

Third, the nature of AI shifts the strategic calculus from retaliation to preemption, inverting the fundamental logic of deterrence. Classic deterrence, particularly in its nuclear variant, is a fundamentally reactive and defensive posture. Its stability rests on a credible second-strike capability, which ensures that even a surprise attack will be met

with devastating retaliation, thus making the initial attack irrational. AI, in contrast, is an adaptive, informational, and preemptive technology (Jackson, 2025). It creates a potential "winner-takes-all" scenario, where the first actor to achieve a decisive breakthrough or execute a successful preemptive cyber or autonomous strike could gain a permanent and insurmountable strategic advantage (Jackson, 2025). This transforms the strategic imperative from "how do I credibly threaten to respond?" to "how do I strike first without being detected?" This is not a mere modification of deterrence; it is its inversion, replacing a logic of prevention with a logic of preemption.

Finally, the opacity of AI capabilities makes the stable balance of power required for deterrence impossible to achieve. The relative transparency of nuclear arsenals, verified through treaties and national technical means, allowed both sides in the Cold War to assess each other's capabilities and maintain a rough equilibrium. AI development, however, occurs behind the closed doors of corporate labs and classified government programs, often concealed as proprietary secrets (Jackson, 2025). It is exceedingly difficult for a state to accurately gauge an adversary's true AI capabilities, leading to worst-case-scenario planning and fueling a destabilizing arms race. Without the ability to clearly perceive and communicate capabilities, a core requirement of deterrence theory cannot be met (Lynch & Morrison, 2023). The result is a strategic environment characterized by profound uncertainty, instability, and a high propensity for miscalculation. A more qualified view is offered by Jensen, Atalan, and Macias (2024), whose crisis simulations found no observable change in participants' overall strategies as AI/ML capabilities varied. They argue that algorithms will reshape the information environment, but human judgment will remain central to crisis management. Table 1 demonstrates the paradigm shift in the strategic logic of the global power dynamics.

Table 1. The Paradigm Shift in Strategic Logic

Feature	Classic Deterrence	Technological Dependence
Key Concepts	Punishment/Denial, Credibility, Rationality	Chokepoint Control, Structural Power, Network Centrality
Primary Instruments	Nuclear Arsenals, Conventional Forces	Export Controls, Standards-Setting, Supply Chains
Strategic Goal	Prevent Attack, Maintain Status Quo	Shape Behavior, Constrain Autonomy
Central Threat	Military Annihilation (Mutually Assured Destruction)	Systemic Disruption (Mutually Assured Disruption)

Source: Author's own elaboration.

The Rise of Structural Power in the Global Tech Stack

As the logic of military deterrence erodes, a new strategic paradigm is emerging, organized around the control of and dependence on critical technologies. The global technology stack, the layered ecosystem of hardware, software, data, and standards that underpins the AI era, has become the central terrain of geopolitical competition. Power in this new arena is derived not from the ability to inflict physical destruction, but from the ability to control access to this ecosystem. This shift requires a corresponding evolution in theoretical understanding, moving from traditional concepts of state power

based on relative capabilities to a more nuanced conception of structural power rooted in the architecture of global technological interdependence.

The Architecture of Interdependence: AI Supply Chains as Strategic Terrain

The geopolitical landscape of the 21st century is being fundamentally reshaped by the intricate and vulnerable supply chains that produce the foundational technologies of the digital age. The semiconductor value chain, in particular, has transformed from a domain of economic optimization into a primary battlefield for great power competition, where strategic control over key nodes can confer decisive advantages.

The semiconductor industry is the bedrock of the modern economy and the engine of artificial intelligence. For decades, its structure was a testament to hyper-globalization, a complex web of international firms specializing in different stages of the production process to maximize efficiency (TokenRing AI, 2025). This efficiency, however, came at the cost of resilience, creating a system that is both hyper-globalized and hyper-concentrated. The result is a supply chain with critical "chokepoints", where a single company or country holds a near-monopolistic position in a vital segment of the production process.

This geographic and corporate concentration is stark. The United States dominates the highest-value stages of the chain, particularly in chip design and the sophisticated Electronic Design Automation (EDA) software that is essential for creating complex integrated circuits (Luo & Van Assche, 2023). Europe, specifically the Dutch firm ASML, holds an absolute monopoly on the Extreme Ultraviolet (EUV) lithography machines required to manufacture the most advanced chips (Luo & Van Assche, 2023). The most capital-intensive stage, fabrication, is dominated by East Asia, with Taiwan's TSMC and South Korea's Samsung controlling the vast majority of the world's advanced logic and memory chip manufacturing capacity (Shukla, 2022).

The strategic realization of these chokepoints, brought into sharp relief by the supply chain disruptions of the COVID-19 pandemic and escalating U.S.-China tensions, has triggered a paradigm shift from efficiency to security (Ha & Lee, 2025). This has given rise to the formation of techno-alliances designed explicitly to control this strategic terrain. The most prominent example is the U.S.-led "Chip 4" alliance, a strategic initiative intended to consolidate the comparative advantages of the United States, Japan, South Korea, and Taiwan across the entire value chain. The alliance's goal is to create a trusted, resilient supply chain among like-minded partners, explicitly to enhance collective economic security and counter China's technological ambitions (Ha & Lee, 2025). This represents a deliberate effort at network re-architecture, moving from an open global system to a politically defined and restricted bloc.

The strategic contest over the semiconductor supply chain is best understood through the framework of weaponized interdependence. This concept describes how states can exploit the asymmetric structures of global networks to gain a strategic advantage (Farrell & Newman, 2019). In a highly interconnected world, power flows to those actors who control the central "hub" nodes through which finance, information, or, in this case, critical technology must pass. States with jurisdiction over these hubs can leverage their

position to coerce other actors who are dependent on access to the network (Farrell & Newman, 2019).

This form of power is exercised through two distinct mechanisms. The first is the panopticon effect, which refers to the ability of the state controlling a hub to use its privileged access to gather information and conduct surveillance on the data and transactions flowing through the network (Farrell & Newman, 2019). The second, and more potent in the context of technology supply chains, is the chokepoint effect. This is the ability to deny adversaries access to the network altogether, effectively cutting them off from the critical flows of goods, services, or data necessary for their economic and military security (Farrell & Newman, 2019). Farrell and Newman (2019) emphasize that network centrality does not automatically produce coercive power. States can exploit hub positions only when they possess both jurisdiction over central nodes and the domestic institutions needed to mobilize them.

The escalating U.S. export controls on advanced semiconductor technology to China are a clear and powerful application of the chokepoint effect. By restricting access not only to finished chips but also to the EDA software and manufacturing equipment necessary to produce them, the United States is leveraging its control over key hubs in the value chain to actively degrade China's ability to develop high-end AI (TokenRing AI, 2025). This strategy demonstrates a fundamental shift in how power is exercised: it is not a threat of future military action, but the immediate and direct manipulation of economic and technological interdependence to achieve strategic objectives. The very structure of the globalized system, once seen as a source of mutual prosperity, has been transformed into an instrument of power politics.

Technological Dependence as Structural Power

To fully grasp the strategic logic of the AI era, it is necessary to move beyond traditional conceptions of power focused on the relative material capabilities of states and embrace a framework centered on structural power. In this new context, the technological "stack" itself constitutes the primary structure of the international system, and the ability to shape this structure, and create dependencies within it, is the ultimate source of influence.

International relations theory has long distinguished between two forms of power. Relational power is the most familiar, corresponding to the ability of actor A to influence the behavior of actor B (Pustovitovskij & Kremer, 2011). This is the power of coercion and inducement, typically measured by comparing the relative military and economic capabilities of states (Kitchen & Cox, 2019). Structural power, by contrast, is a more subtle and profound concept. As defined by Susan Strange, it is "the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic enterprises... have to operate" (Shukla, 2022). It is the power to set the rules of the game, to define the frameworks of interaction, and to change the range of choices available to other actors, often without the need for direct or overt pressure (Shukla, 2022).

Throughout history, technology has been a critical factor in shaping the structure of international relations, from the development of navigation that enabled colonial



expansion to the nuclear revolution that defined the Cold War (Krishna-Hensel, 2010). In the contemporary era, the global technology stack, the integrated ecosystem of hardware (semiconductors), platforms (cloud computing), software (AI frameworks), patents, and technical standards, has become the primary organizing structure of the international system (Danilin, 2018). A state's autonomy, prosperity, and security are now inextricably linked to its position within this structure.

Within this framework, this manuscript formally defines technological dependence as the reliance of an actor on another's technological ecosystem for its own economic viability and national security. This is a multidimensional reliance, encompassing dependence on foreign-designed hardware, foreign-hosted cloud platforms, foreign-developed software frameworks, and internationally-set technical standards (Mayer & Lu, 2025). In this system, dependence is not a bug to be eliminated but a feature to be strategically managed and, for some, exploited.

States that control the foundational layers of this technological stack can be conceptualized as technopoles (Mayer & Lu, 2025). The United States and China are the world's preeminent technopoles, possessing significant technological autonomy and the capacity to "weaponise infrastructure and technologies" by creating and leveraging the dependence of others (Mayer & Lu, 2025). This structural power is exercised through several mechanisms. These can be gathered around the themes of setting standards, controlling chokepoints, and shaping development paths. In the theme of setting standards, dominating the bodies that set global technical standards ensures that the entire ecosystem is optimized for a technopole's domestic industries. In controlling chokepoints, maintaining control over irreplaceable components or software (the chokepoint effect) gives a technopole the ability to grant or deny access to the entire technological system. Finally, in shaping development paths, by embedding other nations within their technological ecosystem, through initiatives like China's Digital Silk Road or the adoption of U.S. cloud platforms, technopoles can shape the developmental trajectory of those nations, making them partners in and dependents of their own techno-political model. Drawing on the Digital Dependence Index, Mayer and Lu (2025) find that many developed and emerging economies face a dual dependence on U.S. platforms and Chinese hardware, leaving them vulnerable to the infrastructural power of both technopoles.

This new reality fundamentally redefines the nature of alliances and sovereignty. Traditional alliances, such as NATO, were security pacts based on mutual defense commitments against military aggression (Rühle, 2015). The new strategic logic, however, is giving rise to technological blocs. Alliances like the Chip 4 are defined not by military treaties but by shared standards, interoperable technologies, and integrated, trusted supply chains (Ha & Lee, 2025). The concept of "friend-shoring", reconfiguring supply chains to align with geopolitical partners, is the economic manifestation of this new alliance structure (Luo & Van Assche, 2023).

Simultaneously, the very meaning of sovereignty is being contested. A state may possess full territorial integrity and political independence in the traditional Westphalian sense, yet lack digital sovereignty if its critical infrastructure, data flows, and digital economy are controlled by foreign entities (Fleming, 2025). The European Union's ambitious "Digital Sovereignty" agenda is an explicit attempt to reclaim sovereign control over this

new, intangible domain, just as China's pursuit of an "independent and controllable" ecosystem is a quest to establish its own digital sovereignty (van Oirsouw, 2024). The most significant conflicts of the future may therefore be fought not over physical territory, but over the control of data, standards, and digital infrastructure.

Strategies of Dependence and Autonomy

The recognition of technological dependence as a form of structural power has prompted the world's major powers, the United States, the European Union, and China, to adopt distinct and competing strategies. Each is attempting to navigate this new strategic landscape by maximizing its own autonomy while shaping the dependencies of others. Their approaches reveal three different models of techno-political organization for the 21st century: a U.S. model based on market-centric network control, an EU model based on regulatory power, and a Chinese model based on state-driven ecosystem construction.

The United States: Architect of the Chokepoint

The United States' strategy is a direct response to the perceived challenge from China and represents a decisive shift away from decades of championing a liberal, market-led international order. The new American approach is one of overt geopolitical techno-nationalism, aimed at leveraging its existing dominance over key chokepoints in the global technology stack to preserve its leadership and constrain its primary rival.

The enactment of the CHIPS and Science Act in 2022 marks a historic pivot in U.S. economic policy. For the first time in decades, the U.S. has embraced a large-scale industrial policy, allocating over $52 billion in federal subsidies to bolster domestic semiconductor manufacturing and research (Blevins et al., 2023). This legislation is not merely an economic stimulus; its purpose is explicitly geopolitical (Luo & Van Assche, 2023). It is designed to reverse the decades-long off-shoring of fabrication capacity, particularly the concentration of advanced manufacturing in East Asia, which U.S. policymakers came to view as a critical national security vulnerability (Blevins et al., 2023).

The Act's core objective is to solidify America's lead in the semiconductor industry while actively containing China's rise (Luo & Van Assche, 2023). By incentivizing the construction of advanced fabrication facilities (fabs) on U.S. soil, the policy aims to reduce dependency on foreign suppliers for the chips that power everything from consumer electronics to advanced military systems (Blevins et al., 2023). This move represents a fundamental break with the logic of market efficiency that previously guided U.S. policy and an embrace of techno-nationalist principles that link technological self-sufficiency directly to state security and geopolitical power (Birkbeck, University of London, 2025).

The CHIPS Act is the domestic component of a broader, more aggressive strategy to weaponize the global semiconductor value chain. Since 2022, U.S. policy has progressively shifted from merely slowing China's technological progress to actively "degrading its peak capabilities" in advanced AI and chip manufacturing (TokenRing AI, 2025). This is achieved by systematically applying the chokepoint effect through a series of escalating export controls.

These controls are unprecedented in their scope, targeting not just the export of advanced AI chips themselves, but also the critical inputs required to produce them. This includes restrictions on the sale of U.S.-origin EDA software, advanced manufacturing equipment, and even the involvement of U.S. citizens and residents in China's semiconductor industry (TokenRing AI, 2025). The strategy is to leverage American dominance in the highest-value, most difficult-to-replicate segments of the supply chain to create a bottleneck that China cannot easily circumvent.

Furthermore, the CHIPS Act itself contains powerful tools of weaponized interdependence. Its "guardrail" provisions prohibit any company, American or foreign, that receives federal funding under the Act from engaging in any significant expansion of advanced semiconductor manufacturing in China for a decade (Luo & Van Assche, 2023). This forces global firms to make a choice: accept U.S. subsidies and decouple their advanced operations from China, or forgo U.S. support and risk being cut out of the emerging U.S.-led technological bloc. This provision effectively coerces a global realignment of the supply chain, forcing a shift away from China and demonstrating a clear use of structural power to alter the range of choices available to other actors. Luo and Van Assche (2023) interpret the CHIPS Act as evidence of a wider shift from market-oriented liberalism to intervention-oriented techno-nationalism, embedding zero-sum geopolitical priorities in global value chains.

The European Union: The Pursuit of Regulatory Sovereignty

The European Union finds itself in a precarious position, caught between the technological dominance of the United States and the rising ambitions of China. Lacking a globally competitive position in many foundational technologies, the EU has adopted a dual-track strategy to assert its influence and achieve "strategic autonomy". This strategy combines the projection of regulatory power to shape global norms with targeted industrial policies aimed at building domestic capacity and reducing critical dependencies.

The EU's primary instrument of structural power is its ability to set global standards through regulation, a phenomenon often termed the "Brussels Effect". The EU AI Act, the world's first comprehensive legal framework for artificial intelligence, is the quintessential example of this strategy in action (van Oirsouw, 2024). The Act employs a risk-based approach, categorizing AI systems from unacceptable risk (which are banned) to high, limited, and minimal risk, with corresponding compliance obligations for each tier (Daly, 2025).

The geopolitical significance of the AI Act lies in its extraterritorial reach. The regulation applies to any provider or deployer placing AI systems on the EU market or whose outputs are used within the EU, regardless of the company's location (Milaninia et al., 2025). Given the size and value of the EU's single market, global technology companies are compelled to comply with its stringent requirements for transparency, risk mitigation, and human oversight. In doing so, the EU effectively exports its regulatory model, shaping global AI development in alignment with its "human-centric" values and establishing itself as a global standard-setter in AI governance (Csernatoni, 2024). This is a deliberate attempt to exercise structural power, not by controlling hardware, but by defining the legal and ethical framework within which all other actors must operate (Daly, 2025). Csernatoni (2024) cautions that regulatory ambition alone cannot secure

European AI leadership, because the EU's limited industrial base, fragmented decision-making, and dependence on U.S.-led AI innovation constrain its pursuit of technological sovereignty.

Alongside its regulatory strategy, the EU has recognized its profound technological dependencies as a critical vulnerability. The bloc relies on non-EU countries for over 80% of its digital products and services, and its share of the global semiconductor manufacturing market has dwindled to below 10% (Knafo, 2025). The EU Chips Act is the bloc's flagship industrial policy designed to reverse this trend and bolster its "Digital Sovereignty" (Fleming, 2025).

The Act mobilizes up to €43 billion in public and private investment with the ambitious goal of doubling the EU's global market share in semiconductors to 20% by 2030 (Timmers, 2022). It is structured around three pillars: the first focuses on research and development to bridge the gap "from lab to fab"; the second aims to attract investment in "first-of-a-kind" manufacturing facilities; and the third establishes a coordination mechanism to monitor the supply chain and respond to crises (ICOS Semiconductors, 2025).

Together, the AI Act and the Chips Act represent the two prongs of the EU's pursuit of strategic autonomy. One seeks to govern the use of technology on a global scale, while the other aims to build the domestic capacity to produce that technology. The overarching goal is to reduce the EU's dependence on both the U.S. and China, allowing it to navigate the emerging techno-political rivalry without being forced to align completely with either bloc, thereby carving out a role as an independent, sovereign pole in the digital age (Bjola, 2021).

China: Forging a Self-Reliant Ecosystem

China's strategy is arguably the most ambitious and state-driven of the three major powers. Confronted with what it perceives as a U.S. campaign to contain its technological rise, Beijing has embarked on a whole-of-nation effort to achieve self-reliance across the entire technology stack. This strategy has both an internal dimension, building a domestic, "independent and controllable" ecosystem, and an external one, exporting its techno-political model to create a parallel, China-centric sphere of influence.

The U.S. export controls have acted as a powerful catalyst for China's self-sufficiency drive, reinforcing Beijing's conviction that dependence on foreign technology is a critical national security risk (Chang et al., 2025). In response, achieving an "independent and controllable" AI ecosystem has become a top national priority, enshrined in policies like the "Made in China 2025" and the "Next-Generation AI Development Plan" (Chang et al., 2025).

This is a state-led effort of immense scale, involving massive public investment through initiatives like the "Big Fund" for semiconductors, which channels billions into strengthening domestic chip manufacturing, design, and materials industries (Chang et al., 2025). The goal is to close the technological gap with the West at every layer of the AI stack. This includes nurturing national champions like Huawei to develop homegrown alternatives to high-end NVIDIA AI chips, as well as promoting the creation of indigenous software frameworks and large language models to reduce reliance on U.S. platforms

(Chang et al., 2025). This strategy is underpinned by the "dual circulation" economic framework, which prioritizes domestic innovation and consumption (internal circulation) to build resilience against external shocks and sanctions, while selectively engaging with global markets (external circulation) (Ali, 2025).

The external-facing component of China's strategy is the Digital Silk Road (DSR), a key pillar of the broader Belt and Road Initiative (BRI) (Reddy, 2023). The DSR is a grand infrastructure project aimed at financing and constructing the digital backbone of the 21st century in partner countries, particularly across the Global South. This includes the deployment of 5G networks, cross-border fiber optic cables, satellite communications, and data centers (Reddy, 2023).

The objectives of the DSR are both commercial and geostrategic. Commercially, it creates new markets for Chinese technology companies like Huawei and ZTE, establishing them as dominant providers of digital infrastructure in emerging economies (Reddy, 2023). Geostrategically, the DSR aims to build a parallel, China-centric digital ecosystem outside the control of the United States (Reddy, 2023). By providing the hardware, software, and technical standards for digitalization in partner nations, Beijing seeks to embed these countries within its sphere of technological influence (Reddy, 2023). This strategy cultivates technological dependence on Chinese systems, promotes norms and standards favorable to China's interests, and ultimately works to reduce global reliance on the U.S.-led digital order, creating a viable alternative for nations to align with.

The distinct approaches of these three powers highlight that the current geopolitical contest is not simply a rivalry between nations, but a competition between fundamentally different models of techno-political organization. The United States is pursuing a market-centric, network-control model, leveraging the power of its private sector and its central position in existing global networks to enforce chokepoints. The European Union is advancing a regulatory-centric, norms-based model, using the power of its large market and legal frameworks to set global standards for technology governance. China, in contrast, is executing a state-centric, infrastructure-building model, using the full power of the state to construct a parallel, vertically integrated technological ecosystem from the ground up. The outcome of this three-way competition will determine the rules, norms, and structure of the global digital order for decades to come.

This competition has also created a dangerous, self-reinforcing dynamic of insecurity-driven innovation. U.S. export controls, intended to enhance American security by slowing China's military modernization, are perceived in Beijing as an existential threat to its national development (Ali, 2025). This profound sense of insecurity is the primary catalyst for China's massive, state-directed push for technological self-sufficiency (Chang et al., 2025). This crash program, in turn, is paradoxically accelerating indigenous Chinese innovation in precisely the areas the U.S. seeks to constrain, which is then perceived in Washington as a growing threat that justifies even more stringent controls (TokenRing AI, 2025). This creates a vicious cycle, a technological security dilemma where the actions each side takes to increase its own security and reduce its dependencies directly decreases the security of the other, fueling an escalatory arms race driven by mutual fear.

Conclusion: The New Security Dilemma, Mutually Assured Disruption

The strategic logic that has governed international security for more than half a century is being fundamentally rewritten. The foundational principles of classic deterrence, built on the threat of military force and the assumption of rational, deliberative human actors, are proving inadequate for an era defined by the algorithmic speed, systemic complexity, and weaponized interdependence of the global technology stack. The central argument of this manuscript is that the paradigm of deterrence has been supplanted by a new strategic logic of dependence. Power is now increasingly derived from the ability to control access to the critical technological ecosystems that form the substrate of modern economic and military strength.

This analysis has demonstrated how the United States, the European Union, and China are each navigating this new reality through distinct strategies aimed at shaping the architecture of global technological interdependence. The United States acts as the architect of the chokepoint, leveraging its historical dominance in key technologies to control and restrict access to the global value chain. The European Union operates as a regulatory superpower, using the gravity of its single market to set global norms and standards for the governance of technology. China is pursuing a grand strategy of self-reliance, attempting to build a parallel, state-centric ecosystem free from foreign dependencies while simultaneously exporting its model through the Digital Silk Road. As a summarizing effort, Table 2 describes the comparative strategies of the great techno-powers.

Table 2. Comparative Strategies of the Great Techno-Powers

Feature	United States	European Union	China
Core Strategic Concept	Chokepoint Control	Regulatory Sovereignty	Self-Reliance & Ecosystem Building
Primary Policy Instruments	CHIPS Act, Export Controls	AI Act, Chips Act, GDPR	Dual Circulation, Digital Silk Road
Source of Power	Network Centrality, Private Sector Dominance	Market Size, Legal Frameworks	State Direction, Public Investment
Ultimate Goal	Maintain Technological Leadership	Set Global Standards, Achieve Strategic Autonomy	Create a Parallel, China-Centric System

Source: Author's own elaboration.

This emerging landscape gives rise to a new and profoundly unsettling security dilemma, one best described as "Mutually Assured Disruption" (MAD). This concept serves as the successor to the Cold War doctrine of Mutually Assured Destruction. In this new paradigm, the ultimate coercive threat is not a nuclear exchange that would physically annihilate an adversary, but rather the ability to sever a rival's access to the foundational technologies of the modern world, to "unplug" a nation from the global tech stack. The weaponization of semiconductor supply chains, the fragmentation of data flows, and the balkanization of technical standards all point to a future where the most potent form of attack is systemic economic and societal disruption.

The rise of techno-nationalism, while a rational response by states seeking to enhance their resilience and security, carries immense risks (Malone, 2024). It threatens to fragment the global technology ecosystem, which could stifle the very innovation that drives progress, increase costs for all, and create a more volatile and unpredictable international system. The vicious cycle of insecurity-driven innovation, where each power's attempt to secure its own technological base is perceived as a threat by others, fuels an escalatory spiral with no clear off-ramp.

The central challenge for policymakers in the coming decades will be to manage the inherent tension of this new era. Interdependence is simultaneously a critical vulnerability to be mitigated and an unavoidable reality of a globally integrated technology ecosystem. The final, pressing question is whether the great powers can develop new norms, confidence-building measures, and adaptive security strategies to manage the profound risks of Mutually Assured Disruption (miniOrange, 2025). Or, is the world destined for a permanent state of techno-geopolitical rivalry behind a new, and perhaps more dangerous, Silicon Curtain? The answer will determine the future of international peace and security in the 21st century.

References

AUSA. (2020, February 12). *AI, robots could make it harder to deter conflict*. Association of the United States Army. https://www.ausa.org/news/ai-robots-could-make-it-harder-deter-conflict

Ali, G. (2025). China's strive for self-reliance in advanced technology. *China-US Focus*. https://www.chinausfocus.com/peace-security/chinas-strive-for-self-reliance-in-advanced-technology

Al Midfa, N. (2025). China's AI strategy: A case study in innovation and global ambition. *Trends Research & Advisory*. https://trendsresearch.org/insight/chinas-ai-strategy-a-case-study-in-innovation-and-global-ambition/

Bjola, C. (2021). *The European Union's quest for digital sovereignty and its implications for the Transatlantic relationship* (Working Paper No. 5). Oxford Digital Diplomacy Research Group. http://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/DigDiploROxWP5.pdf

Birkbeck, University of London. (2025, March 20). *Techno-nationalism and geopolitical risk – Prospects for the US/China relationship (CIMR debates in Public Policy)* [Event]. Centre for Innovation Management Research. https://www.bbk.ac.uk/events/event/47156/techno-nationalism-and-geopolitical-risk-ndash-prospects-for-the-us-china-relationship-cimr-debates-in-public-policy

Blevins, E. G., Grossman, A. B., & Sutter, K. M. (2023). *Semiconductors and the CHIPS Act: The global context* (CRS Report No. R47558). Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R47558

Chang, W., Arcesati, R., & Hmaidi, A. (2025). *China's drive toward self-reliance in artificial intelligence: From chips to large language models*. Mercator Institute for China Studies. https://merics.org/en/report/chinas-drive-toward-self-reliance-artificial-intelligence-chips-large-language-models

Chow, P. C. (2025). Chip-Four Alliance for a resilient global semiconductor industry. In *Technology rivalry between the USA and China* (pp. 269–307). Springer Nature Switzerland.

Csernatoni, R. (2024). *Charting the geopolitics and European governance of artificial intelligence*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence?lang=en

Daly, K. (2025). The geopolitics of AI regulation. *The Yale Review of International Studies*. https://yris.yira.org/global-issue/the-geopolitics-of-ai-regulation/

Danilin, I. V. (2018). *Emerging technologies and their impact on international relations and global security*. Hoover Institution. https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security

Dohmen, H. (2024). *Assessing China's AI development and forecasting its future tech priorities*. Atlantic Council. https://www.atlanticcouncil.org/content-series/strategic-insights-memos/assessing-chinas-ai-development-and-forecasting-its-future-tech-priorities/

Elbashir, M. (2024). EU AI Act sets the stage for global AI governance: Implications for US companies and policymakers. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/geotech-cues/eu-ai-act-sets-the-stage-for-global-ai-governance-implications-for-us-companies-and-policymakers/

European Chips. (2025). *Chips Act: Updates, compliance, training*. https://www.european-chips-act.com/

European Commission. (2025). *European Chips Act*. Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-chips-act

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79.

Fleming, S. (2025). What is digital sovereignty and how are countries approaching it? *World Economic Forum*. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

Ha, B., & Lee, T. C. (2025). The Chip 4 Alliance and technological geopolitics: Taiwan and South Korea's economic security responses. *Taiwan International Studies Quarterly, 21*(3), 79–117.

ICOS Semiconductors. (2025). *Strategy: EU Chips Act*. ICOS—Chips for Europe Initiative. https://icos-semiconductors.eu/strategy-eu-chips-act/

Jackson, M. (2025). Why AI deterrence will fail: The case against mutual assured AI malfunction (MAIM). *Medium*. https://medium.com/@shaheim/why-ai-deterrence-will-fail-the-case-against-mutual-assured-ai-malfunction-maim-2dd901c7dafa

Jensen, B., Atalan, Y., & Macias, J. M., III. (2024). *Algorithmic stability: How AI could shape the future of deterrence*. Center for Strategic and International Studies. https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence

Kassenova, N., & Duprey, B. (2021). *Digital Silk Road in Central Asia: Present and future*. Davis Center for Russian and Eurasian Studies. https://daviscenter.fas.harvard.edu/research-initiatives/program-central-asia/digital-silk-road-central-asia-present-and-future

Kitchen, N., & Cox, M. (2019). Power, structural power, and American decline. *Cambridge Review of International Affairs, 32*(6), 734–752.

Knafo, S. (2025). *Report on European technological sovereignty and digital infrastructure* (A10-0107/2025, 2025/2007(INI)). Committee on Industry, Research and Energy, European Parliament. https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

Krishna-Hensel, S. F. (2010). Technology and international relations. In *Oxford research encyclopedia of international studies*.

Larsen, B. C. (2022). *The geopolitics of AI and the rise of digital sovereignty*. Brookings Institution. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

Luo, Y., & Van Assche, A. (2023). The rise of techno-geopolitical uncertainty and international business: Implications of the United States Chips and Science Act. *Journal of International Business Studies, 54*, 1423–1440.

Lynch, J., & Morrison, E. (2023). *Deterrence through AI-enabled detection and attribution* (Kissinger Center Paper). Henry A. Kissinger Center for Global Affairs, Johns Hopkins School of Advanced International Studies. https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/deterrence-through-ai-enabled-detection-and-attribution/

Malone, M. R. (2024). Techno-nationalism trend fuels global disorder. *University of Miami News*. https://news.miami.edu/stories/2024/10/techno-nationalism-trend-fuels-global-disorder.html

Mayer, M., & Lu, Y. C. (2025). Global structures of digital dependence and the rise of technopoles. *New Political Economy*, 1–20.

Mazarr, M. J. (2018). *Understanding deterrence* (Perspective No. PE-295). RAND Corporation. https://www.rand.org/pubs/perspectives/PE295.html

Milaninia, N., O'Brien, A. C., Vermynck, E.-C., Helleputte, C., & Boggs, J. C. (2025). *Transatlantic AI governance, strategic implications for U.S., EU compliance*. King & Spalding. https://www.kslaw.com/news-and-insights/transatlantic-ai-governance-strategic-implications-for-us-eu-compliance

miniOrange. (2025). *What is adaptive security? Benefits, use cases & examples*. https://www.miniorange.com/blog/what-is-adaptive-security/

Moreira, D. K. (2019). The limits of classic and perfect deterrence theory: A game-theory analysis of the United States-North Korea nuclear standoff. *The Yale Review of International Studies*. https://yris.yira.org/essays/the-limits-of-classic-and-perfect-deterrence-theory-a-game-theory-analysis-of-the-united-states-north-korea-nuclear-standoff/

Optica. (2023). *EU Chips Act*. Optica Public Policy. https://www.optica.org/get_involved/public_policy/chips_initiatives/eu_chips_act/

Pustovitovskij, A., & Kremer, J. (2011). *Structural power and international relations analysis: "Fill your basket, get your preferences."* Ruhr-Universität Bochum Institute of Development Research and Development Policy.

Quackenbush, S. L. (2011). Deterrence theory: Where do we stand? *Review of International Studies, 37*(2), 741–762.

Reddy, R. K. (2023). *Digital Silk Road*. ORCA Asia. https://www.orcasia.org/digital-silk-road

Rühle, M. (2015, April 20). Deterrence: What it can (and cannot) do. *NATO Review*. https://www.nato.int/docu/review/articles/2015/04/20/deterrence-what-it-can-and-cannot-do/index.html

Shukla, S. (2022). Revisiting structural power in the global economy: It's multinationals, not states. *Journal of International Affairs, 75*(1). https://jia.sipa.columbia.edu/content/revisiting-structural-power-global-economy-its-multinationals-not-states

SIPRI. (2020). *International cooperation in a new era of techno-nationalism* [Webinar]. Stockholm International Peace Research Institute Stockholm Security Conference 2020. https://www.sipri.org/events/2020/SSC20-international-cooperation-era-techno-nationalism

Timmers, P. (2022). How Europe aims to achieve strategic autonomy for semiconductors. *Brookings Institution*. https://www.brookings.edu/articles/how-europe-aims-to-achieve-strategic-autonomy-for-semiconductors/

TokenRing AI. (2025, November 3). The new silicon curtain: Geopolitics reshapes global chip supply and the future of AI. *Financial Content*. https://markets.financialcontent.com/stocks/article/tokenring-2025-11-3-the-new-silicon-curtain-geopolitics-reshapes-global-chip-supply-and-the-future-of-ai

van Oirsouw, T. (2024). *AI, digital sovereignty, and the EU's path forward: A case for mission-oriented industrial policy*. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School. https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/

WebAsha Technologies. (2025). *Adaptive security strategy in 2025: A continual defense approach against evolving cyber threats*. WebAsha Technologies Blog. https://www.webasha.com/blog/adaptive-security-strategy-a-continual-defense-approach-against-evolving-cyber-threats

Wong, Y. H., Yurchak, J., Button, R. W., Frank, A. B., Laird, B., Osoba, O. A., Steeb, R., Harris, B. N., & Bae, S. J. (2020). *Deterrence in the age of thinking machines* (Research Report No. RR-2797). RAND Corporation. https://www.rand.org/pubs/research_reports/RR2797.html

Zagare, F. C. (2022). Perfect deterrence theory. In *Russian studies, political science, and the philosophy of technology* (p. 335). Bloomsbury Publishing.