POLITICS & SECURITY
ISSN 2815-3324 Online, ISSN 2535-0358 Print

THE GEOPOLITICS OF CYBERSECURITY: A COMPARATIVE ANALYSIS OF NATIONAL STRATEGIES FOR DIGITAL SOVEREIGNTY

Oksana Prokopyshyn
Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies Lviv
Lviv, Ukraine
https://orcid.org/0000-0002-7027-3499

Nataliia Trushkina
Research Center for Industrial Problems of Development of the NAS of Ukraine
Kharkiv, Ukraine
https://orcid.org/0000-0002-6741-7738

Abstract. *This paper investigates the divergent national strategies for achieving "digital sovereignty" among four major geopolitical actors: the United States, the European Union, China, and Russia. It argues that digital sovereignty has evolved from a defensive concept focused on network security into a comprehensive geopolitical strategy for projecting power, values, and economic influence (Süsslin, 2025; Metakides, 2025). Through a comparative analysis of key policy and legal frameworks—including the US National Cybersecurity Strategy (2023), the EU's GDPR/DSA/DMA package, China's Cybersecurity Law (CSL), and Russia's "Sovereign Internet" laws—the paper identifies three distinct models of digital sovereignty: the US market-driven, rebalanced-responsibility model; the EU's regulation-as-power, normative model; and the Sino-Russian state-centric, control-oriented model (Metakides, 2025; Freedom House, n.d.). The analysis reveals that these approaches are creating a fragmented "splinternet," characterized by competing regulatory blocs, contested data governance regimes, and a securitized global technology supply chain (Carnegie Endowment for International Peace, 2025). The paper concludes by proposing a new framework that understands digital sovereignty not merely as a quest for autonomy but as a primary vector for exercising state power in a multipolar digital world order, with significant implications for global stability, international law, and the future of the internet..*

Keywords: Digital Sovereignty, Geopolitics, Cybersecurity, Splinternet, Data Governance, US National Cybersecurity Strategy, EU GDPR, China Cybersecurity Law, Russia Sovereign Internet.

1. INTRODUCTION: THE RISE OF DIGITAL SOVEREIGNTY IN A FRACTURING CYBERSPACE

The early architecture of the internet was animated by a utopian vision of a borderless, global commons—a space for open communication, innovation, and connection that would transcend the physical constraints of the nation-state (The White House, 2023). This vision, however, has been progressively fractured. The contemporary digital ecosystem is a contested domain, increasingly defined by geopolitical tensions, the weaponization of synthetic media, and the normalization of cyber-enabled conflict (Center for Long-Term Cybersecurity, 2025; Palo Alto Networks, 2025). The result is not a single, global internet but an accelerating fragmentation into multiple "splinternets": a collection of isolated or semi-isolated networks controlled by governments, each with its own rules, standards, and values (Carnegie Endowment for International Peace, 2025). This trend signals a profound global shift in which, as some analysts have noted, "digital solidarity is out. Tech sovereignty is in" (Carnegie Endowment for International Peace, 2025).

This fragmentation is a direct consequence of states reasserting control over the digital sphere through the pursuit of "digital sovereignty." As a concept, digital sovereignty is both polysemic and politically charged (e.g., Couture & Toupin, 2019). At its core, it refers to the ability of a state or collective community to exercise control and autonomy over its digital infrastructure, data flows, and the foundational technologies that underpin its economy and society (e.g., Couture & Toupin, 2019; Süsslin, 2025). This pursuit is not necessarily for complete technological self-sufficiency but for strategic autonomy in critical areas to protect national interests, security, and economic prosperity (Süsslin, 2025). The concept is now mobilized by a diverse range of actors, from liberal democracies seeking to protect citizens' rights to authoritarian states aiming to consolidate control, making it a central battleground in 21st-century geopolitics (e.g., Couture & Toupin, 2019; Metakides, 2025).

The impetus for this global turn towards digital sovereignty is deeply rooted in a pervasive sense of geopolitical insecurity. The digital domain has become a primary theater for great power competition, and the shockwaves of terrestrial conflicts are felt acutely in cyberspace (Munich Security Conference, 2022; Palo Alto Networks, 2025). The Russian invasion of Ukraine, for instance, was accompanied by cyberattacks and sparked widespread fears of digital escalation against NATO states, heightening distrust between geopolitical blocs (Munich Security Conference, 2022). In this "tumultuous moment in history," where the rules-based international order is under assault, digital dependencies have transformed from assets into profound vulnerabilities (Munich Security Conference, 2022; Institute for Defense Analyses, 2023). The push to erect "digital walls" (Carnegie Endowment for International Peace, 2025) and build digital fortresses is a direct response to this volatility, representing a state's attempt to regain a measure of security and predictability in an environment where its digital lifelines are exposed to foreign manipulation and disruption.

This paper advances the thesis that national strategies for digital sovereignty are not merely reactive, technical cybersecurity policies. They are proactive, comprehensive geopolitical projects that reflect and project distinct ideological values, economic models, and visions of world order. These strategies represent a fundamental reassertion of the state in the digital age, challenging the once-dominant multi-stakeholder model of internet governance (ResearchGate, 2021). By conducting a comparative analysis of the strategic approaches of the United States (US), the European Union (EU), the People's Republic of of China (PRC), and the Russian Federation, this paper will demonstrate how these competing visions are actively shaping the future of cyberspace (Metakides, 2025; Freedom House, n.d.). It will argue that these divergent paths are creating a multipolar digital world, with profound implications for international law, global trade, and the very architecture of the internet.

2. THEORETICAL FRAMEWORK: SOVEREIGNTY, POWER, AND REGULATION IN THE DIGITAL AGE

To analyze the complex interplay of forces shaping national digital sovereignty strategies, this paper employs a multidisciplinary theoretical framework drawing from International Relations (IR), law, political economy, and Science and Technology Studies (STS) (Martino & Gamal, 2022). This framework provides the analytical lens to deconstruct and compare the divergent approaches of the US, EU, China, and Russia.

The analysis is grounded in the classical concept of Westphalian sovereignty, which posits the state's exclusive and supreme authority within its defined territorial boundaries (Werthner, 2025). The central debate in the geopolitics of cybersecurity revolves around whether and how this principle can be extended into the intangible, non-territorial realm of cyberspace (Werthner, 2025; Süsslin, 2025). This question frames the fundamental ideological clash between the state-centric model of governance, championed by China and Russia, and the multi-stakeholder model, historically promoted by the United States and civil society organizations (Süsslin, 2025; ResearchGate, 2021). The former sees the internet as a space to be governed by sovereign states to protect national security and public order, while the latter envisions a decentralized ecosystem managed by a diverse group of actors, including industry, academia, and non-governmental organizations (ResearchGate, 2021).

To understand the EU's unique strategy, this paper utilizes the concepts of "regulatory mercantilism" and the "Brussels Effect" (Süsslin, 2025; PromethEUs, 2023). Regulatory mercantilism describes how states use regulations, standards, and certifications not only for domestic policy goals but also as tools of economic and geopolitical competition (Süsslin, 2025). The "Brussels Effect" is a specific manifestation of this, whereby the EU leverages its large, attractive single market to externalize its legal and regulatory norms globally (PromethEUs, 2023). Landmark regulations like the General Data Protection Regulation (GDPR) compel multinational corporations to adopt EU standards worldwide to access the European market, effectively allowing the EU to project power and shape global business practices without resorting to traditional military or economic coercion (PromethEUs, 2023). This makes regulation itself a primary instrument of the EU's pursuit of digital sovereignty.

For China's approach, the framework of "rule by law" provides a critical distinction from the Western concept of the "rule of law" (U.S.-China Economic and Security Review Commission, 2023). In a "rule by law" system, law is not an independent constraint on state power but rather a primary instrument for the ruling party—in this case, the Chinese Communist Party (CCP)—to implement its policies and achieve its strategic objectives (U.S.-China Economic and Security Review Commission, 2023). This includes maintaining social control, directing economic development, and projecting influence internationally. This legal philosophy is inextricably linked to the rise of techno-authoritarianism, where the state deploys advanced surveillance and control technologies, justified and enabled by a comprehensive legal architecture. China actively exports this governance model through initiatives like the Digital Silk Road, offering technology and training to other nations, thereby shaping global norms to reflect its own state-centric, control-oriented vision (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023).

Finally, adopting a perspective from STS, this paper views sovereignty not merely as an abstract legal claim but as a tangible reality that is actively constructed, or "infrastructured" (Musiani et al., 2019). Digital sovereignty is realized through the co-construction of policy, legal frameworks, technical standards, and physical infrastructures. To understand a nation's strategy, one must analyze not only its laws and doctrines but also the material components that enforce them: the development of national data centers, control over encryption standards and internet routing protocols, and the management of the physical conduits of data flow like subsea cables and data ports (Musiani et al., 2019; MERICS, 2023).

A nation's approach to digital sovereignty is thus best understood as an inseparable trinity of its technological capacity, its legal-regulatory philosophy, and its core political ideology. These three elements are mutually constitutive and cannot be analyzed in isolation. The EU's relative weakness in the platform economy, for example, necessitates its heavy reliance on regulatory power to govern the dominant US and Chinese tech giants—a form of asymmetric statecraft (PromethEUs, 2023; McKinsey & Company, 2022). Conversely, China's ability to implement its "Great Firewall" and comprehensive surveillance systems depends on possessing both the legal mandate from its Cybersecurity Law and the indigenous technological capacity of companies like Huawei and Alibaba to build and operate these systems (U.S.-China Economic and Security Review Commission, 2023; MERICS, 2020). The law justifies the technology, the technology enforces the law, and both serve the CCP's ideological goal of comprehensive control. This integrated trinity forms the fundamental unit of analysis for comparing the national strategies that follow.

3. COMPARATIVE ANALYSIS OF NATIONAL STRATEGIES FOR DIGITAL SOVEREIGNTY

The divergent paths taken by the United States, the European Union, China, and Russia in their pursuit of digital sovereignty have given rise to distinct, and often conflicting, models of digital governance (Couture & Toupin, 2019; Freedom House, n.d.). These models are not merely technical frameworks but are deeply embedded in each actor's unique political culture, economic structure, and geopolitical ambitions. An examination of their core doctrines and key legal instruments reveals a fragmenting global digital order.

Table 1: A Comparative Framework of National Digital Sovereignty Strategies

Dimension	**United States**	**European Union**	**People's Republic of of China**	**Russian Federation**
Core Doctrine	Market-Driven Security & Rebalanced Responsibility (The White House, 2023)	Normative Power & Strategic Autonomy (Metakides, 2025; PromethEUs, 2023)	Cyber Sovereignty & Comprehensive State Control (Cheng & Liu, 2022; Freedom House, n.d.)	Defensive Sovereignty & Digital Fortress (ResearchGate, 2021)
Key Legal/Policy Instruments	National Cybersecurity Strategy (2023) (The White House, 2023), CLOUD Act (The Belfer Center for Science and International Affairs, 2021), Sector-specific regulations (Süsslin, 2025)	GDPR, Digital Services Act (DSA), Digital Markets Act (DMA), AI Act, NIS2 Directive (PromethEUs, 2023; European Parliament, 2025)	Cybersecurity Law (CSL), Data Security Law (DSL), PIPL, "Great Firewall" (MERICS, 2023; Freedom House, n.d.)	"Sovereign Internet Law," (ResearchGate, 2021) Data Localization Laws (FZ-242) (Gorodissky & Partners, 2023)
Primary Goal	National & Economic Security (Galinec et al., n.d.)	Protection of Fundamental Rights & Single Market Integrity (PromethEUs, 2023; European Parliament, 2025)	Regime Stability & Social Control (U.S.-China Economic and Security Review Commission, 2023; Freedom House, n.d.)	Regime Stability & Insulation from External Pressure (ResearchGate, 2021; Freedom House, n.d.)
Approach to Data Governance	Sector-specific, market-led, with a shift towards federal privacy law (The White House, 2023; Süsslin, 2025)	Comprehensive, rights-based, extraterritorial ("Brussels Effect") (Süsslin, 2025; PromethEUs, 2023)	State-centric, data as a national asset, strict localization (MERICS, 2023)	Strict data localization, state control over data flows (Gorodissky & Partners, 2023)
Stance on Global Internet Governance	Historically multi-stakeholder, now with a stronger emphasis on national interest and security (U.S.-China Economic and Security Review Commission, 2023; The White House, 2023)	Multi-stakeholder, but shaped by EU values and regulations (PromethEUs, 2023)	State-centric, promoting "cyber sovereignty" at the UN/ITU (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023)	State-centric, actively disrupting the multi-stakeholder model (ResearchGate, 2021)

3.1. THE UNITED STATES: A MARKET-DRIVEN ECOSYSTEM WITH REBALANCED RESPONSIBILITY

The US approach to cybersecurity and digital sovereignty has historically been characterized by a reliance on market forces, public-private partnerships, and a sector-specific regulatory model (The White House, 2023; SIPRI, 2024). The 2023 National Cybersecurity Strategy (NCS) represents a significant evolution of this approach, introducing a new philosophy centered on two fundamental shifts: rebalancing responsibility and realigning incentives (Institute for Defense Analyses, 2023; The White House, 2023). This strategy explicitly recognizes that the burden of cybersecurity has fallen disproportionately on individual users and small organizations (The White House, 2023). It seeks to shift this responsibility to the actors most capable of bearing it: large-scale technology providers and the owners and operators of critical infrastructure (The White House, 2023).

The strategy is structured around five pillars that operationalize this vision (Institute for Defense Analyses, 2023; The White House, 2023; Galinec et al., n.d.; Federal Communications Commission, 2023):

1. Defend Critical Infrastructure: This involves expanding the use of minimum cybersecurity requirements for critical sectors and strengthening public-private collaboration (The White House, 2023).
2. Disrupt and Dismantle Threat Actors: This calls for a more proactive, integrated use of all instruments of national power—diplomatic, military, intelligence, and law enforcement—to make malicious cyber activities costly and unsustainable for adversaries (The White House, 2023).
3. Shape Market Forces to Drive Security and Resilience: This is arguably the most innovative pillar. It proposes using federal procurement power and potential legislation to shift liability onto providers of insecure software products and services, thereby creating powerful market incentives for building security in by design (The White House, 2023).
4. Invest in a Resilient Future: This pillar focuses on long-term investments in a secure technical foundation for the internet, R&D for next-generation technologies like post-quantum cryptography, and strengthening the national cyber workforce (The White House, 2023; Galinec et al., n.d.).
5. Forge International Partnerships to Pursue Shared Goals: This reaffirms the US commitment to working with allies to build coalitions, strengthen partner capacity, and reinforce global norms of responsible state behavior (The White House, 2023).

The US strategy is lauded in expert assessments for its forward-thinking vision on aligning private-sector incentives with security goals and for its robust framework for public-private partnerships (The Belfer Center for Science and International Affairs, 2025). However, it is also criticized for significant gaps, particularly in its lack of specific measures to protect individuals, their personal data, and vulnerable small- and medium-sized enterprises (SMEs) (The Belfer Center for Science and International Affairs, 2025). Geopolitically, the NCS is explicit, naming China as the "broadest, most active, and most persistent threat" and framing the global digital competition as a contest of values (The White House, 2023). It champions a vision of an "open, free, global, interoperable, reliable, and secure" internet (The White House, 2023; Institute for Defense Analyses, 2023). Yet, this official stance exists in tension with recent political trends suggesting a potential pivot towards a more transactional, "America First" approach to technology policy, which could prioritize American primacy over the principles of digital solidarity and international cooperation (Carnegie Endowment for International Peace, 2025).

3.2. THE EUROPEAN UNION: SOVEREIGNTY THROUGH NORMATIVE POWER AND REGULATION

The European Union has carved out a distinct "third way" in the global digital order, one that is neither the market-led model of the US nor the state-controlled model of China (Couture & Toupin, 2019; Metakides, 2025). The EU's strategy is to achieve "strategic autonomy" and "digital sovereignty" through the exercise of its formidable regulatory power (PromethEUs, 2023; Metakides, 2025). This approach is born from a clear-eyed assessment of its geopolitical position: while the EU is an economic heavyweight, it lacks homegrown technology giants on the scale of those in the US and China (McKinsey & Company, 2022). Consequently, it leverages its most powerful asset—its unified, high-value single market—to set the rules of the game for all actors who wish to operate within it (Süsslin, 2025; PromethEUs, 2023).

The EU's regulatory arsenal is comprehensive and continues to expand:

- The General Data Protection Regulation (GDPR) is the backbone of this strategy. Enacted in 2018, it established a global "gold standard" for data protection, centering on the fundamental rights of individuals (PromethEUs, 2023). Its extraterritorial scope forces companies worldwide to comply with EU norms, demonstrating the "Brussels Effect" in action (Süsslin, 2025; PromethEUs, 2023).

- The Digital Services Act (DSA) and Digital Markets Act (DMA), which became fully applicable in 2024, extend this regulatory reach to the largest online platforms, designated as "gatekeepers" (e.g., European Parliament, 2025; Hausfeld, 2022; European Commission, n.d.). The DSA imposes new responsibilities for content moderation to create a safer online environment, while the DMA introduces pro-competitive rules to ensure fairness and contestability in digital markets, directly targeting the business models of non-EU tech giants (PromethEUs, 2023; European Parliament, 2025; Hausfeld, 2022).
- The AI Act and Cyber Resilience Act represent the next wave of this strategy, embedding regulatory requirements into emerging technologies from the outset. The AI Act establishes a risk-based framework for artificial intelligence, while the Cyber Resilience Act mandates security standards for all products with digital elements (PromethEUs, 2023; European Parliament, 2025).

Underpinning these laws is a coherent data governance strategy aimed at creating "sovereign data ecosystems" (PromethEUs, 2023). The Data Governance Act (DGA) and the Data Act (DA) establish frameworks for increasing trust and facilitating data sharing within and between sectors, envisioning common European data spaces for health, energy, and public administration (PromethEUs, 2023). This is a deliberate effort to foster a data-driven European economy that operates according to EU values of privacy, security, and fairness (PromethEUs, 2023; European Data Protection Supervisor, 2025).

3.3. CHINA: CYBER SOVEREIGNTY AS AN INSTRUMENT OF COMPREHENSIVE STATE CONTROL

China's approach to the digital domain is the most explicit and comprehensive articulation of state-centric control. Its guiding doctrine is "cyber sovereignty" (网络主权, wǎngluò zhǔquán), which posits that cyberspace is a domain of national sovereignty, equivalent to land, sea, and air, and therefore subject to the absolute authority of the state (U.S.-China Economic and Security Review Commission, 2023; ResearchGate, n.d.; Cheng & Liu, 2022). This doctrine is not primarily about protecting individual rights but about safeguarding national security, ensuring social stability, and cementing the political power of the CCP (U.S.-China Economic and Security Review Commission, 2023).

This doctrine is operationalized through a powerful legal triad:

- The Cybersecurity Law (CSL) of 2017 is the foundational legislation. It establishes broad, and often vaguely defined, security obligations for "network operators" and "critical information infrastructure operators" (CIIOs), giving the state extensive powers of supervision and inspection (ResearchGate, n.d.; Cheng & Liu, 2022; Süsslin, 2025; Freedom House, n.d.; Alkan, 2012).
- The Data Security Law (DSL) of 2021 builds on the CSL by creating a hierarchical system for data classification. Data is categorized based on its importance to national security and public interest, with the strictest controls applied to "national core data" and "important data" (MERICS, 2023).
- The Personal Information Protection Law (PIPL) of 2021 is China's analogue to the GDPR. While it grants individuals rights regarding their personal data, these rights are subordinate to the state's interests (Süsslin, 2025). The law contains broad national security exemptions and mandates state access to data, reflecting the "rule by law" philosophy where individual rights are granted by the state and can be curtailed for state purposes (Süsslin, 2025; U.S.-China Economic and Security Review Commission, 2023).

The enforcement of this legal regime relies on two powerful mechanisms: the "Great Firewall" and strict data localization requirements. The Great Firewall is far more than a simple censorship tool; it is a sophisticated system for controlling the entirety of China's digital environment, managing cross-border data flows, filtering content, and blocking access to foreign services (Carnegie Endowment for International Peace, 2025; MERICS, 2023; Mirrlees, 2022). This is complemented by stringent data localization rules under the CSL and DSL, which mandate that all personal information and "important data" generated within China must be stored on domestic servers (MERICS, 2023). This ensures the state has unfettered access to and jurisdiction over the data, effectively creating a "state-controlled data island"

(MERICS, 2023). China actively exports this model of cyber governance globally through its Digital Silk Road initiative and by providing training and technology to officials from other countries, promoting an alternative, authoritarian vision for the future of the internet (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023).

3.4. RUSSIA: THE SOVEREIGN INTERNET AS A DEFENSIVE DIGITAL FORTRESS

Russia's strategy for digital sovereignty is primarily defensive and, in many respects, isolationist. It is driven by a deep-seated fear of Western political and cultural influence, the potential for foreign-instigated "color revolutions," and a paramount desire to ensure regime stability (ResearchGate, 2021; Freedom House, n.d.). The overarching goal is to insulate the Russian domestic internet segment, known as the "Runet," from external pressures and to guarantee its continued operation even in the event of a disconnection from the global internet (Litvinenko, 2021; ResearchGate, 2021).

The centerpiece of this strategy is the "Sovereign Internet Law" (Federal Law No. 90-FZ), which came into force in 2019 (ResearchGate, 2021). This legislation mandates the creation of a national Domain Name System (DNS) to reduce reliance on international servers. More critically, it requires all domestic internet traffic to be routed through state-controlled exchange points managed by the telecommunications regulator, Roskomnadzor (ResearchGate, 2021). This provides the state with the technical infrastructure necessary to monitor, filter, block, and potentially isolate the Runet from the outside world, creating a "digital fortress."

Like China, Russia enforces strict data localization rules. Federal Law No. 242-FZ, enacted in 2015, requires that any company, foreign or domestic, that collects the personal data of Russian citizens must store and process that data on servers physically located within the Russian Federation (Gorodissky & Partners, 2023; Hivenet, n.d.; Captain Compliance, 2025). This law is a clear assertion of jurisdictional sovereignty, ensuring that the data of its citizens remains within the legal reach of Russian authorities and security services (Hivenet, n.d.). Non-compliance has led to significant fines and the blocking of services like LinkedIn (Gorodissky & Partners, 2023).

While Russia and China are often grouped together as proponents of state-centric "digital sovereignty," their approaches have notable differences (ResearchGate, 2021). Russia's strategy is less technologically and economically integrated than China's. It is more narrowly focused on control and insulation, reflecting a less developed domestic technology sector and a more confrontational diplomatic posture (ResearchGate, 2021; Freedom House, n.d.; U.S. Department of State, 2023). In international forums, Russia often plays the role of the primary disruptor of the multi-stakeholder model, while China pursues a more patient, long-term strategy of building an alternative ecosystem and sphere of influence (ResearchGate, 2021).

4. DISCUSSION: THEMATIC CONTESTS IN THE GEOPOLITICS OF CYBERSPACE

The implementation of these divergent national strategies is not occurring in a vacuum. They collide in key arenas of the global digital ecosystem, creating new forms of geopolitical contestation. The battle for digital sovereignty is being waged over data flows, through global supply chains, and in the race for technological supremacy.

4.1. THE BATTLE FOR DATA: FLOWS VS. FORTRESSES

At the heart of the geopolitical struggle is a fundamental conflict over the governance of cross-border data flows. This contest pits models that favor the free, albeit regulated, flow of data against those that prioritize data localization and state control. The EU's GDPR exemplifies a conditional flow model, permitting data transfers only to jurisdictions that provide an "adequate" level of protection, effectively exporting its standards (PromethEUs, 2023). The US has historically advocated for a more liberal, market-driven approach to data flows, though this is increasingly being tempered by national security concerns (Süsslin, 2025).

In stark contrast, China and Russia have erected digital fortresses built on strict data localization mandates (MERICS, 2023; Gorodissky & Partners, 2023). These policies require that citizen data and other categories of "important data" be stored domestically, which serves the dual purpose of asserting sovereign jurisdiction and ensuring state access for security and surveillance purposes (Hivenet, n.d.; The Belfer Center for Science and International Affairs, 2021). This approach is often justified on grounds of protecting national security and citizen privacy from foreign surveillance (Hivenet, n.d.). However, critics argue that such measures are often a tool for digital authoritarianism, enabling greater government control over information and stifling dissent (Hivenet, n.d.). Economically, data localization can impose significant costs, increase regulatory complexity, and handicap innovation by creating barriers to the global data exchange that fuels modern business (The Belfer Center for Science and International Affairs, 2021). This clash of data governance philosophies is a primary driver of the internet's fragmentation, creating a "balkanized" global landscape where data cannot move freely across competing regulatory blocs (PromethEUs, 2023).

4.2. THE SECURITIZATION OF GLOBAL SUPPLY CHAINS

The competition for digital sovereignty has expanded beyond data and software to encompass the physical hardware and supply chains that form the backbone of the digital world. Advanced technologies, particularly semiconductors, are no longer viewed merely as commercial products but as "sovereign assets" fundamental to national security (Center for Long-Term Cybersecurity, 2025). This has led to the deep securitization of global technology supply chains.

The US has been at the forefront of this trend, with policies like the CHIPS and Science Act and escalating sanctions against China's technology industry. These are not just economic measures; they are explicit national security strategies designed to slow China's technological advancement and secure US leadership in critical technologies (Center for Long-Term Cybersecurity, 2025; Mirrlees, 2022). This approach is not unique to the US. The EU, China, and Russia are all implementing measures to vet, limit, or prohibit foreign hardware and software in their critical infrastructure and government systems (SIPRI, 2024). China's "document 79" initiative, for example, reportedly aims to replace foreign technology in state-owned enterprises, while Russia has banned foreign software from its critical infrastructure facilities (SIPRI, 2024). The EU's NIS2 Directive and other regulations include provisions for assessing supply chain risks, including the potential for "undue influence by a third country on suppliers" (SIPRI, 2024). This transforms international trade in technology into a key battleground of geopolitical competition, where trust is low and every component is potentially suspect.

4.3. THE RACE FOR TECHNOLOGICAL SUPREMACY: AI AND QUANTUM

Emerging and foundational technologies, especially artificial intelligence (AI) and quantum computing, represent the new high ground in geopolitical competition. Leadership in these fields is seen as essential not only for future economic prosperity but also for national security and military advantage (Center for Long-Term Cybersecurity, 2025; Winslow, 2025; World Health Organization, 2020). The rapid advancement of these technologies has triggered a global race for supremacy, with enormous stakes.

This race is unfolding across multiple dimensions. Nations are pouring vast resources into R&D, as seen in the US strategy's call to reinvigorate federal research and China's massive state-backed investments (The White House, 2023; Creemers, 2020; National Development and Reform Commission, 2021). They are also developing divergent approaches to governance. The EU is pioneering a risk-based, human-centric regulatory model with its AI Act, seeking to ensure that AI development aligns with democratic values (PromethEUs, 2023; European Parliament, 2025). In contrast, China's approach is state-driven, focused on rapid deployment for economic gain and social management, integrating AI into its surveillance and control apparatus (U.S.-China Economic and Security Review Commission, 2023; MERICS, 2020). The geopolitical implications are profound, as these technologies can be used to power sophisticated cyberattacks, conduct influence operations with deepfakes, or achieve decisive military superiority (Center for Long-Term Cybersecurity, 2025; Winslow, 2025; Belli, 2025). The looming threat of a cryptographically relevant quantum computer—one capable of breaking current encryption standards—adds another layer of urgency, forcing nations to prepare for a "post-quantum future" where today's secure data could become transparent (The White House, 2023; Center for Long-Term Cybersecurity, 2025; KPMG, 2025).

This intense pursuit of digital sovereignty, while intended to bolster national security, is paradoxically cultivating new and systemic global vulnerabilities. The fragmentation of the internet into distinct "splinternets" and "data islands" dramatically increases the complexity of the global digital ecosystem (Carnegie Endowment for International Peace, 2025; MERICS, 2023; Winslow, 2025). This complexity is not merely an inconvenience; it is a source of strategic risk. As multinational corporations are forced to splinter their data systems to comply with a patchwork of conflicting regulations, the operational overhead and potential for error increase (MERICS, 2023). This environment fosters a "cyber inequity," where smaller organizations, often critical links in global supply chains, lack the resources to navigate the complex regulatory landscape and maintain robust security, creating weak points that adversaries can exploit (Winslow, 2025). Furthermore, in a crisis, the lack of interoperability and shared norms between these fragmented blocs would severely hamper a coordinated international response to a major cyber incident. The digital walls built for defense could easily become the walls of a prison, isolating nations and making it harder to fight a common, sophisticated threat. The very architecture of fragmentation creates seams and gaps, and in the "fog of war" of a major cyber conflict, these seams are precisely where catastrophic failures are most likely to occur (Palo Alto Networks, 2025).

5. CONCLUSION: PROJECTING POWER IN A DIVIDED DIGITAL FUTURE

The evidence and analysis presented in this paper demonstrate that the concept of "digital sovereignty" has undergone a critical evolution. It has transformed from a primarily defensive posture, concerned with protecting national networks from external threats, into a proactive and increasingly offensive instrument for projecting national power in the 21st century. The strategies of the world's major digital actors are no longer just about building firewalls; they are about exporting influence, values, and economic models. The European Union projects its power through normative regulation, using the "Brussels Effect" to shape global markets in its image (PromethEUs, 2023). China projects its power by exporting its techno-authoritarian governance model via the Digital Silk Road, creating a sphere of influence aligned with its state-centric vision (ResearchGate, 2021; U.S.-China Economic and Security Review Commission, 2023). The United States continues to project power through the global dominance of its technology industry and its ability to shape market standards, now coupled with a more explicit strategy of leveraging market forces and liability to enforce security (The White House, 2023; Mirrlees, 2022).

This reality necessitates moving beyond the simplistic "open vs. closed" binary that has long dominated discussions of internet governance. The Cold War-era dichotomy of a free and "open" internet (led by the US and the West) versus a censored and "closed" internet (led by China and Russia) is no longer sufficient to describe the global landscape (Center for Long-Term Cybersecurity, 2025). The emergence of the EU as a distinct regulatory superpower has created a multipolar digital order with at least three competing poles (Metakides, 2025). The EU's model is neither fully open in the libertarian, market-led sense of the US, nor is it fully closed in the authoritarian, state-controlled sense of China. It represents a third, values-driven, regulatory-heavy approach that is actively shaping the behavior of the other two (Metakides, 2025; PromethEUs, 2023).

In this new multipolar digital world, the strategic alignment of "digital middle powers"—nations like India, Brazil, Nigeria, and Indonesia—becomes a decisive factor (Pannier, 2023). These countries are not just passive recipients of technology and norms; they are increasingly influential actors in their own right. Their strategic choices—which model to emulate, which standards to adopt, or whether to forge their own hybrid approaches—will determine the future balance of power in global digital governance. The competition for their allegiance is the new geopolitical prize, and their decisions will shape the contours of the splinternet for decades to come.

The scientific novelty of this paper lies in its reframing of digital sovereignty not as a niche cybersecurity issue, but as a primary instrument of 21st-century statecraft, integrating legal, technological, economic, and ideological dimensions of power (Werthner, 2025). It provides a framework for understanding how states are competing to define the future of a digital world that is no longer global and unified, but fragmented and contested. This analysis opens several critical avenues for future research. First, there is a pressing need for empirical studies on how digital middle powers are navigating this geopolitical competition and formulating their own sovereign strategies (Pannier, 2023). Second, the fragmentation of the digital sphere requires the development of new international legal principles and diplomatic mechanisms for managing conflict and ensuring stability in a world without a single, universally accepted set of rules. Finally, continued analysis of the long-term impact of the technological race, especially in AI and quantum computing, is essential for understanding its potential to either stabilize or destabilize the international system (Center for Long-Term Cybersecurity, 2025). The choices made today will determine whether the divided digital future is one of managed competition or perpetual conflict.

REFERENCES

Alkan, M. (2012). Cybersecurity governance models: A brief overview. *Information & Security: An International Journal, 38*(2), 58–66.

Arsène, S. (2019). The turn to sovereignty in internet governance. In F. Musiani, S. Arsène, C. O. de la Sablière, & C. T. (Eds.), *The turn to sovereignty in internet governance*.

BDO. (2024, September). *Top cybersecurity threats and predictions for 2025*.

Belli, L. (2025). *Cybersecurity and AI*.

Bendiek, A., & Scholl, P. (2024). The EU's strategic turn in cybersecurity: a case of regulatory mercantilism?. *International Affairs, 100*(6), 2379-2397.

Captain Compliance. (2025, January 6). *Russia Data Localization Law: 2025 Essential Guide*.

Carnegie Endowment for International Peace. (2025, May). *Digital democracy in a divided global landscape*.

Carroll, J. M. (2024). Secure Your Supply Chains: A Recipe for Building the Best Products. *Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024*.

Center for Long-Term Cybersecurity (CLTC), UC Berkeley. (2025). *Reflections on cybersecurity futures 2025: Looking back from the present*.

China Aerospace Studies Institute. (2021, October). *U.S.-China Competition in AI*.

Cleary Gottlieb. (2022, October 27). *Digital Services Act Published in the EU Official Journal*. Cleary Antitrust Watch.

Couture, S., & Toupin, S. (2019). What does the notion of "digital sovereignty" stand for? A comparison of the terms used in the public debates of Canada, China, France, and Russia. *New Media & Society, 21*(10), 2319-2337.

Creemers, R. (2020). *China's approach to cyber sovereignty*. Konrad Adenauer Stiftung.

Davis Center for Russian and Eurasian Studies, Harvard University. (2021). *Digital Silk Road in Central Asia: Present and Future*.

European Commission. (n.d.). *The Digital Services Act*. Retrieved July 3, 2025, from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

European Data Protection Supervisor (EDPS). (2025, March). *EDPS Mandate Review 2020–2024*.

European Liberal Forum. (2023). *The Digital Services Act (DSA): Between European autonomy and transatlantic cooperation*.

European Parliament. (2025, April). *Digital agenda for Europe*.

European Parliament. (2025). *The Recovery and Resilience Facility (RRF) and cybersecurity*.

European Union. (2022a). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union, L 265*, 1-66.

European Union. (2022b). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union, L 277/1*.

Federal Communications Commission. (2023, July). *National Cybersecurity Strategy*.

Freedom House. (n.d.). *Freedom on the Net Reports*.

Future of Privacy Forum. (2022, June). *Chinese Data Protection in Transition*.

Google Cloud. (2025). *Cybersecurity Forecast 2025*.

Gorodissky & Partners. (2023). *Data protection in the Russian Federation: overview*.

Government of Malta. (2023). *Maltese National Cybersecurity Strategy 2023-2026*.

Hausfeld. (2022, November 1). *The EU Digital Markets Act*.

Hernández, S., & Raina, A. (2020). Legal problems with data localization requirements: The case of the Russian Federation. *Global Trade and Customs Journal, 15*(9), 445–459.

Hivenet. (n.d.). *Does national pride win over innovation? The contradictions in data localization*.

Hunton Andrews Kurth LLP. (2023). *2023 Data Protection and Privacy: Introduction*.

Institute for Defense Analyses. (2023). *Summary of National Cybersecurity Strategy with Similarity Analysis to Executive Order 14028*.

International Trade Administration. (n.d.). *Challenges of the Chinese eCommerce Market*. U.S. Department of Commerce.

James Cook University. (2020). *Research Data & Information Management Framework 2020-2025*.

KPMG. (2025, June). *Cyber considerations 2025*.

Lee, T.-L. (2025, February). Digital health governance: Technological solutionism, human rights, and data sovereignty. *European Journal of Legal Studies, Special Issue*, 101-159.

Martino, L., & Gamal, N. (Eds.). (2022). *European Cybersecurity in Context*. European Liberal Forum.

McKinsey & Company. (2022, September). *Securing Europe's competitiveness: Addressing its technology gap*.

McKinsey Global Institute. (2022, January). *The data-driven enterprise of 2025*.

MERICS. (2020, June). *China's digital rise*.

MERICS. (2023, November). *The future of the internet: How China is shaping the infrastructure of tomorrow*.

Metakides, G. (2025). A crucial decade for European sovereignty. In *Perspectives on Digital Humanism*.

Middle East Institute. (2023). *The 2023 National Cybersecurity Strategy: How does America think about cyberspace?*

Mirrlees, T. (2022). Sanctioning China's Tech Industry to 'Secure' Silicon Valley's Global Dominance. In *The Geopolitical Economy of Communications and Digital Technology*.

MS.codes. (2023). *US National Cybersecurity Strategy 2023*.

Munich Security Conference. (2022). *Munich Cyber Security Conference 2022 SpringForum Report*.

Musiani, F., et al. (2025, March 11). Infrastructuring digital sovereignty: A research agenda. *Frontiers in Communication*.

National Development and Reform Commission, PRC. (2021, May). *14th Five-Year Plan (2021-2025) for National Economic and Social Development and the Long-Range Objectives Through the Year 2035*.

Old Dominion University. (2023, November 5). *General Review of the National Cybersecurity Strategy March 2023*.

Palo Alto Networks. (2025). *Navigating the geopolitical cybersecurity landscape in 2025*.

Pannier, A. (2023). *Digital Middle Powers and the Global Tech Competition*. Institut français des relations internationales (ifri).

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4).

Precisely & Drexel University's LeBow College of Business. (2024). *2025 Outlook: Data Integrity Trends and Insights*.

PromethEUs. (2023, June). *The EU Data Strategy: The new EU framework for data flows and its international implications*.

Republic of Bulgaria. (2021). *National Cybersecurity Strategy "Cyber Resilient Bulgaria 2025" (Draft Translation)*.

ResearchGate. (2021, June). *Digital Silk Road in Central Asia: Present and Future for Russian and Eurasian Studies*. Davis Center for Russian and Eurasian Studies, Harvard University.

Royal United Services Institute (RUSI). (n.d.). *New ways to frame responsible state behaviour in cyberspace*.

SIPRI. (2024, June). *Cyber risk reduction in China, Russia, the United States and the European Union*.

Süsslin, L. E. (2025, February). *Digital Sovereignty and Geopolitics in the Field of Data Protection: A Comparison of the EU, China, and the USA*.

The Belfer Center for Science and International Affairs, Harvard Kennedy School. (2021, July). *Sovereignty and Data Localization*.

The Belfer Center for Science and International Affairs, Harvard Kennedy School. (2025, March). *Cybersecurity Strategy Scorecard*.

The White House. (2023, March). *National Cybersecurity Strategy*.

Threat Intelligence. (2024). *2025 Cybersecurity Trends*.

Tzogopoulos, G. (2021, November). *The Digital Markets Act (DMA): Between European autonomy and transatlantic cooperation*. ELIAMEP.

U.S.-China Economic and Security Review Commission. (2023, November). *China's increasingly global legal reach*.

U.S. Department of State. (2023, March). *2022 Country Reports on Human Rights Practices: Russia*.

Van De Grift, S. C. (2019). *A Comparative Analysis of the State of Digital Rights in China, Russia, the United States, and Germany*. Rollins Scholarship Online.

Werthner, H. (2025). Geopolitics, digital sovereignty, what's in a word. In *Perspectives on Digital Humanism*.

Winslow, E. (2025, January). *Global Cybersecurity Outlook: A complex cyberspace in 2025*. World Economic Forum.

World Bank. (2021). *Cybersecurity in the financial sector: A digest of regulatory guidance*.

World Health Organization. (2020). *Global strategy on digital health 2020–2025*.

Zenkina, S. (2021). Institutional aspects of Russia's transition to the sixth technological structure: political incentives, economic barriers and environmental impact. *E3S Web of Conferences, 258*, 05037.