International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(5s) 2026 pp. 390-409
https://doi.org/10.70917/ijcisim-2026-2719
Article

Digital and Technological Sovereignty in the Age of Strategic Competition: Implications for Security and Defense

Roger Sanz Gonzalez[1], Claudio Paya Santos[2], Juan Carlos Fernández-Rodríguez[3], Neidy Zenaida Domínguez Pineda[4], Rosa Vera García[5], Rafael Canorea-García[6]

[1] Valencian International University, Spain.
Email: rsanzg@professional.universidadviu.com
ORCID: 0009-0006-1419-2367
[2] Valencian International University, Spain.
Email: claudio.paya@professor.universidadviu.com
ORCID: 0000-0002-1908-9960
[3] Isabel I of Castile University, Spain.
Email: juancarlos.fernandez9227@ui1.es
ORCID: 0000-0003-3312-861X
[4] Valencian International University, Spain.
Email: neidyz.dominguez@professor.universidadviu.com
ORCID: 0000-0002-8574-2606
[5] Center for Higher Education in Teaching and Educational Research (CEIE), Spain.
Email: rosa.vera@cardenalcisneros.es
ORCID: 0000-0001-8040-6382
[6] ESIC University, Spain.
Email: rafael.canorea@esic.university
ORCID: 0000-0002-6637-4369
Corresponding Author:Claudio Paya Santos,claudio.paya@professor.universidadviu.com

Abstract: The transformation of digital and technological sovereignty from abstract concepts to operational imperatives marks a defining feature of contemporary international security. This comprehensive analysis examines how states navigate the intersection of digital governance and technological autonomy in an era characterized by intensifying strategic competition, supply chain vulnerabilities, and the weaponization of interdependence. Drawing on recent developments through 2025, we analyze divergent sovereignty models across major powers and regions—the European Union's normative-regulatory approach, the United States' security-industrial paradigm, China's state-centered control model, Russia's defensive isolation strategy, and emerging hybrid frameworks in the Indo-Pacific and Latin America. The study reveals that while convergence exists in recognizing sovereignty as essential for strategic autonomy, fundamental divergences persist in normative foundations, policy instruments, and security implications. For defense communities, these sovereignty dynamics reshape military planning, alliance structures, and deterrence strategies, suggesting that the future security architecture will be determined by how states reconcile autonomy aspirations with the inescapable realities of technological interdependence.
Keywords: digital sovereignty, cybersecurity, defense policy, semiconductors, artificial intelligence, digital governance

Introduction

The accelerating convergence of digital transformation and geopolitical rivalry has elevated sovereignty concerns from peripheral policy debates to the core of national security strategy. Recent global disruptions—including

semiconductor shortages, cyberattacks on critical infrastructure, and the strategic use of technology export controls—have demonstrated that digital and technological dependencies constitute acute vulnerabilities in the contemporary security environment. The European Union's 2025 State of the Digital Decade report emphasizes structural reforms to bolster technological and economic sovereignty, particularly in connectivity and public service delivery, while China's semiconductor industry has made rapid strides despite U.S. export controls, with companies like Huawei developing advanced semiconductors and 5G infrastructure by 2024.

This transformation reflects a fundamental shift in the nature of power and security. Unlike traditional sovereignty, which centered on territorial control and political independence, digital and technological sovereignty encompasses the capacity to govern data flows, secure cyber infrastructures, maintain industrial bases for critical technologies, and shape global technical standards. These capabilities increasingly determine states' ability to project power, maintain strategic autonomy, and protect national interests in an interconnected yet fragmented global order (Mazurier et al., 2019).

The urgency of sovereignty concerns has intensified dramatically since 2022. The Russia-Ukraine conflict exposed the vulnerability of states dependent on foreign technology, while U.S.-China technological competition has accelerated, with Chinese competitors remaining approximately five years behind global leaders in high-volume manufacturing of leading-edge logic semiconductor chips according to August 2024 assessments. Meanwhile, only 16% of European respondents in Wire's 2025 European Sovereignty Survey were optimistic that Europe would achieve digital sovereignty within the next five years, highlighting the gap between aspirations and capabilities.

This article provides a comprehensive analysis of how digital and technological sovereignty are conceptualized, operationalized, and contested across major powers and regions. We examine the theoretical foundations distinguishing digital from technological sovereignty, analyze diverse regional approaches and their security implications, and assess the impact on defense planning, alliance dynamics, and strategic competition. The analysis draws on recent policy developments, academic literature, and empirical evidence through September 2025 to offer defense and security professionals a framework for understanding sovereignty's role in shaping the emerging international order.

1. Theoretical Framework

1.1 Reconceptualizing Sovereignty for the Digital Age

The traditional Westphalian conception of sovereignty—supreme authority within territorial boundaries and independence in external relations—faces fundamental challenges in the digital domain. Cyberspace operates across borders, data flows transcend jurisdictions, and private technology corporations wield influence comparable to states. This reality necessitates reconceptualizing sovereignty for conditions where territorial control provides limited leverage over digital processes and technological capabilities that determine economic competitiveness and military effectiveness (Jiang et al., 2024; Kello, 2024).

Actual research discussion identifies three evolutionary phases in digital sovereignty discourse. The first phase (2010-2015) emphasized defensive reactions to revelations about surveillance programs and platform dominance. The second phase (2016-2020) witnessed proactive articulation of sovereignty doctrines, exemplified by Europe's GDPR and China's cybersecurity laws (Delgado et al., 2023). The current third phase (2021-present) integrates sovereignty into comprehensive strategies linking digital governance, industrial policy, and national security (Bendiek & Stürzer, 2023; Timmers, 2024)

1.2 Digital Sovereignty: Governance in Cyberspace as a key factor

Digital sovereignty encompasses the capacity to exercise effective authority over digital infrastructures, data resources, and cyberspace governance within a state's sphere of influence. Recent conceptual refinements identify four operational dimensions (Couture & Toupin, 2024; Floridi, 2023):

1.2.1 **Data Sovereignty**

Data sovereignty refers to the authority of states or communities over the collection, processing, storage, and transfer of data. In the digital economy, data is the foundational resource that underpins innovation, competitiveness, and national security. The principle of data sovereignty ensures that sensitive information remains subject to the jurisdiction of the country where it is generated, preventing strategic dependence on foreign entities. For example, the European Union’s General Data Protection Regulation (GDPR) operationalizes data sovereignty by setting strict conditions on cross-border data flows (European Commission, 2021). This sovereignty dimension also encompasses

critical debates on cloud infrastructures, digital platforms, and the balance between economic efficiency and privacy protection (Couture & Toupin, 2019; Pohle & Thiel, 2020).

1.2.2 **Infrastructure Sovereignty**

Infrastructure sovereignty concerns ownership and governance of digital infrastructures such as telecommunications networks, cloud services, and digital platforms (Mazurier et al., 2019). These infrastructures represent the backbone of economic and security systems, and dependence on external providers creates vulnerabilities in both strategic autonomy and resilience. The COVID-19 pandemic and semiconductor shortages exposed the risks of fragile or externally dominated infrastructures, accelerating policies like the European Chips Act or U.S. reshoring initiatives (Farrell & Newman, 2019, 2024). Infrastructure sovereignty therefore demands investments in domestic or trusted supply chains, diversification of providers, and the development of indigenous cloud and network solutions to secure continuity of essential services (Edler et al., 2023).

1.2.3 **Algorithmic Sovereignty**

Algorithmic sovereignty denotes the capacity of a state or society to design, regulate, and control artificial intelligence systems and automated decision-making processes (Payá et al 2025). As AI increasingly determines outcomes in sectors ranging from healthcare and finance to defense and cybersecurity, sovereignty in this domain is critical to ensure transparency, accountability, and alignment with societal values (Floridi, 2023). Without algorithmic sovereignty, states risk ceding authority to opaque systems developed by foreign corporations or adversarial actors (Zuboff, 2023). The EU's AI Act exemplifies an attempt to establish algorithmic sovereignty by classifying AI systems by risk and enforcing compliance with ethical standards (European Parliament, 2025). This dimension directly shapes the balance between innovation, public trust, and security in the deployment of AI technologies.

1.2.4 **Regulatory Sovereignty**

Regulatory sovereignty refers to the ability of states to define and enforce legal and normative frameworks governing digital environments. It includes the protection of fundamental rights, cybersecurity obligations, competition policies, and the standard-setting processes that influence global technology governance. Through regulatory sovereignty, states can project influence beyond their borders, as demonstrated by the so-called "Brussels effect," where EU digital regulations become de facto global standards (Bradford, 2023). This aspect of sovereignty not only reinforces national autonomy but also creates avenues for international leadership by shaping the global rules of the digital order (Bendiek & Stürzer, 2023).

1.3 *Future spaces of technological Sovereignty*

The evolution toward "algorithmic sovereignty" reflects growing recognition that AI systems constitute critical governance infrastructure. As Zuboff (2023) argues, the ability to shape algorithmic processes determines not only economic outcomes but also social and political possibilities. This expanded conception links digital sovereignty directly to democratic governance and human rights protection.

Must be taken in consideration quantum computing sovereignty that refers to the capacity of a state to design, produce, and control quantum technologies—particularly quantum computers, communication systems, and cryptographic solutions—without critical dependence on external actors. Unlike conventional digital infrastructures, quantum technologies are expected to fundamentally alter the balance of power in computing, cybersecurity, and defense. A breakthrough in quantum capabilities could render classical encryption obsolete, accelerate artificial intelligence training, and transform scientific research and military planning (Payá et al., 2018; 2023).

This dimension of sovereignty is not only about securing access to quantum hardware but also about developing the ecosystem of **software, algorithms, talent, and standards** that underpin quantum innovation. The United States, the European Union, and China are currently leading the race, with massive public investment programs such as the EU's *Quantum Flagship*, the U.S. *National Quantum Initiative Act*, and China's multi-billion-dollar national quantum research centers (European Commission, 2025; U.S. Congress, 2018; Lee, 2024). These initiatives reveal that quantum computing sovereignty is being framed as a strategic asset on par with semiconductors or artificial intelligence (Payá et al., 2025).

At the defense level, quantum sovereignty intersects with **national security** in two main ways: (1) ensuring that adversaries cannot compromise communications or critical infrastructures through quantum-enabled cyberattacks, and (2) gaining first-mover advantages in quantum sensing and navigation for military applications (Scharre, 2023).

Sovereignty in this domain therefore requires not only technological investments but also **international coordination of standards and norms** to avoid destabilizing security dilemmas in a rapidly evolving field.

1.4 Technological Sovereignty: Material Foundations of Autonomy

Technological sovereignty is not a modern concept raised on twenty first century. In fact, this domain is a constant evolution of sovereignty that denotes the ability to develop, produce, and maintain control over critical technologies essential for economic competitiveness, national security, and societal resilience. Recent frameworks emphasize five core components (Edler et al., 2023; March & Schieferdecker, 2024):

Technological sovereignty may be defined as the capacity of states to develop, produce, and exert control over critical technologies that underpin economic competitiveness, national security, and societal resilience. Far from representing an aspiration to autarky, the notion is increasingly articulated as a strategic framework designed to guarantee autonomy within conditions of global interdependence (Edler et al., 2023). Its analytical value lies in identifying the essential pillars that enable states and regional organizations to reduce strategic dependencies while sustaining long-term innovation and resilience (March & Schieferdecker, 2024).

A first component is **innovation capacity**, understood as the sustained ability to conduct frontier research and translate results into technological applications. This dimension is strongly conditioned by the level of public investment in science, the density of research networks, and the effectiveness of public–private partnerships. Initiatives such as the European Union's *Horizon Europe* programme or the United States' *CHIPS and Science Act* illustrate how governments seek to institutionalize innovation ecosystems as critical levers of sovereignty (European Commission, 2025; U.S. Congress, 2022). Without such capacity, states risk being confined to the role of consumers rather than producers of transformative technologies, particularly in fields such as artificial intelligence, biotechnology, and quantum computing (Sanz et al., 2024: Gangi, 2025).

The **industrial base** constitutes a second dimension. It refers to domestic manufacturing capabilities in strategic sectors, including semiconductors, advanced batteries, and telecommunications infrastructure. Strengthening the industrial base has become a priority in light of the vulnerabilities revealed by global supply chain disruptions and rising geopolitical tensions. The European Chips Act and China's extensive investment in semiconductor fabrication plants demonstrate how industrial policy has been reframed as a strategic instrument of sovereignty (European Commission, 2025; Lee, 2024). Industrial capacity thus represents a material foundation for technological independence and resilience.

Closely related is **supply chain resilience**, the third component. The COVID-19 pandemic underscored the fragility of highly globalized production systems, particularly in relation to semiconductors and critical raw materials. Resilience in this domain requires diversification of suppliers, the establishment of regional hubs, and the development of monitoring mechanisms to anticipate disruptions. The United States has incorporated supply chain resilience into its National Defense Strategy, while India's *Semicon India* programme seeks to position the country as a regional center for electronics production (Pant & Taneja, 2024). This dimension highlights that sovereignty in practice depends less on complete independence than on the ability to manage interdependence under adverse conditions.

A fourth dimension is **standards authority**, which refers to the capacity of states to influence or determine international technical standards. Control over standards not only enables the diffusion of domestic norms but also consolidates long-term influence over global markets. The European Union exemplifies this phenomenon through the so-called "Brussels Effect," whereby instruments such as the GDPR or the forthcoming AI Act establish regulatory benchmarks with global repercussions (Bradford, 2023; Bendiek & Stürzer, 2023). Conversely, China's *Standards 2035* strategy illustrates an alternative attempt to institutionalize national preferences at the international level (State Council of China, 2023). Standards authority thus constitutes both a geopolitical instrument and a mechanism of value projection.

Finally, **human capital** emerges as the decisive factor that sustains all other components. The availability of highly qualified personnel in science, technology, engineering, and mathematics (STEM) fields conditions the effectiveness of innovation systems, industrial bases, and regulatory capacity. Initiatives such as Japan's *Society 5.0* and the European Union's *Digital Education Action Plan* demonstrate the centrality of workforce development in strategies of technological autonomy (Hemmings, 2024; European Commission, 2025). In the absence of robust human capital, technological sovereignty remains fragile, regardless of financial investment or regulatory ambition.

Taken together, these five dimensions—innovation capacity, industrial base, supply chain resilience, standards authority, and human capital—constitute an interdependent framework. Each dimension reinforces the others, creating

a virtuous cycle in which innovation strengthens industrial capacity, industrial production enhances supply chain security, resilient supply chains underpin standards influence, and all are sustained by the development of human expertise. Technological sovereignty, therefore, should not be interpreted as a retreat into isolation, but rather as the pursuit of **strategic autonomy within interdependence**, enabling states to navigate the dual logics of competition and cooperation in the evolving global technological order (March & Schieferdecker, 2024).

The semiconductor sector exemplifies technological sovereignty challenges. The U.S. aims to increase domestic chip production from 12% in 2022 to 20% by 2024 through government subsidies and private sector investments, while China's CXMT has grown its global DRAM market share from near zero in 2020 to about 5% in 2024, demonstrating how sovereignty drives industrial transformation.

1.5 Theoretical Convergence and Divergence

Contemporary theories of sovereignty reveal both convergent and divergent trajectories in the digital-technological domain. **Convergence** is evident in the nearly universal recognition that control over digital infrastructures and critical technologies has become a prerequisite for maintaining strategic autonomy, irrespective of political regime or economic model (Floridi, 2020; Edler et al., 2023). States across the globe acknowledge that vulnerabilities in data governance, supply chains, or technological standards directly undermine national resilience, economic competitiveness, and defense capabilities (Mazurier et al., 2019).

At the same time, significant **divergences** emerge in how sovereignty is conceptualized and pursued. **Liberal-democratic models** tend to frame sovereignty as a means to safeguard individual rights, maintain market competition, and reinforce rules-based governance frameworks (Mazurier et al., 2019). Within this paradigm, sovereignty does not imply isolation, but rather the establishment of regulatory mechanisms—such as the GDPR or the AI Act—that protect rights while fostering trust in digital ecosystems (Bradford, 2023; Bendiek & Stürzer, 2023). The underlying assumption is that sovereignty can coexist with openness, provided that robust safeguards and enforceable norms are in place.

By contrast, **state-centric models** emphasize governmental authority and national security imperatives. Sovereignty here is closely linked to centralized control of digital infrastructures and the securitization of cyberspace. China's "cyberspace sovereignty" doctrine and Russia's efforts to develop a sovereign internet exemplify this orientation, where the state positions itself as the ultimate arbiter of technological infrastructures and digital flows (Epifanova, 2023; Standing Committee of the NPC, 2021). In these models, sovereignty is operationalized as an instrument of regime stability and geopolitical leverage.

Developmental models prioritize sovereignty as a tool for capacity-building and inclusive growth. This perspective is particularly salient in emerging economies, where digital infrastructures are leveraged to expand access, reduce inequalities, and promote regional cooperation. Latin America's debates on digital sovereignty, for example, emphasize developmental goals such as bridging the digital divide, fostering local innovation, and reducing dependence on foreign platforms (Aguerre, 2024; Belli, 2023). Sovereignty in this sense is not primarily about geopolitical competition, but about harnessing digital technologies for sustainable development and social inclusion.

Finally, **hybrid models** attempt to reconcile multiple objectives by selectively integrating elements of the aforementioned paradigms. India illustrates this approach by combining strong state leadership in building digital public infrastructures (such as Aadhaar and UPI) with market-driven innovation and commitments to democratic oversight (Pant & Taneja, 2024; Rajmohan et al., 2025). Similarly, Japan balances openness to international alliances with efforts to strengthen its own industrial base and regulatory capabilities (Hemmings, 2024). Hybrid models thus reveal the flexibility of sovereignty as a strategic framework, shaped by the interplay between national imperatives and global interdependence.

These theoretical divergences translate directly into distinct **policy approaches and security strategies**, ranging from regulatory projection and international norm-setting to protective isolationism and developmental cooperation. Understanding these differences is critical to analyzing how states pursue technological autonomy and how competing models affect the prospects for global cooperation or fragmentation in the digital age (Farrell & Newman, 2019, 2024).

1.6 Sovereignty as Strategic Autonomy

Digital and technological sovereignty are frequently subsumed under the broader concept of strategic autonomy, particularly in European debates. Strategic autonomy refers to the capacity of political communities to act

independently in international affairs, free from external coercion or excessive dependency. In this sense, digital and technological sovereignty are operational domains of strategic autonomy (Floridi, 2020).

In defense terms, sovereignty in these domains underpins deterrence, resilience, and operational freedom. States that cannot secure their digital infrastructures or maintain control over critical technologies risk losing sovereignty in the broader sense: they become dependent clients in global power hierarchies.

1.7 Academic and Policy Debates

The academic literature offers competing interpretations of sovereignty in the digital and technological realms:

2 Critical perspectives argue that sovereignty discourses are often used by states to justify digital authoritarianism or protectionist policies (Mueller, 2020).

3 Constructivist approaches emphasize that sovereignty is socially constructed, varying across regions and shaped by cultural values (Couture & Toupin, 2019).

4 Pragmatic policy analyses focus on the tools and instruments by which sovereignty is pursued—regulation, industrial subsidies, cyber defense strategies, and international agreements (Pohle & Thiel, 2020; Edler et al., 2023).

The policy sphere reflects these tensions. While the EU frames digital sovereignty around individual rights and democratic values, China frames it as cyberspace sovereignty aligned with state authority. The U.S. prioritizes supply chain resilience and industrial leadership, while Russia interprets sovereignty as control over information flows within a sovereign internet (Standing Committee of the NPC, 2021; State Council of China, 2023; White House, 2021). Latin America, India, and Japan articulate hybrid models balancing development, openness, and national security (OECD, 2020; Rajmohan et al., 2025; Shiozawa, 2022).

1.8 Theoretical Relevance for Security and Defense

From a defense and security perspective, the theoretical framework underscores several key insights:

- Sovereignty is multidimensional: States must simultaneously address legal, technical, industrial, and strategic dimensions.
- Dependencies equal vulnerabilities: Over-reliance on foreign technologies or platforms exposes defense systems to espionage, sabotage, or coercion.
- Normative competition: Divergent models of digital and technological sovereignty reflect broader ideological competition, influencing alliances and adversarial relations.
- Dynamic processes: Sovereignty is not an absolute condition but a constantly renegotiated balance between openness, interdependence, and control.

Thus, understanding digital and technological sovereignty is not only an academic exercise but a strategic necessity for defense policymakers.

2. Regional and National Approaches to Digital and Technological Sovereignty

2.1 European Union: Normative Power Through Regulatory Leadership

The European Union's strategy on digital and technological sovereignty has evolved considerably since 2022, shifting from a primarily defensive posture to an increasingly proactive effort to shape global digital governance. This transition is anchored in the recognition that economic competitiveness, societal resilience, and security are deeply intertwined with control over digital infrastructures and critical technologies (Bendiek & Stürzer, 2023). The European Parliament's 2025 report on technological sovereignty highlights the necessity of reinforcing financial instruments under the forthcoming Multiannual Financial Framework (MFF) in order to expand semiconductor production capacities and foster next-generation technologies (European Parliament, 2025). In this context, sovereignty is framed not as isolation but as a strategy of "open strategic autonomy," combining regulatory leadership with international cooperation (European Commission, 2025).

2.1.1 Recent Policy Developments

The EU's approach crystallized through a sequence of landmark initiatives that collectively define its "sovereignty through regulation" strategy. The **European Chips Act (2023)** mobilized approximately €43 billion in

public and private investments to secure semiconductor supply chains and reduce dependency on external suppliers (European Commission, 2023). The **Data Act (2024)** established frameworks for industrial data sharing, aiming to unlock innovation while ensuring fair competition and interoperability (European Commission, 2024). The **AI Act (2024)** represented the world's first comprehensive regulatory framework for artificial intelligence, positioning the EU as a global standard-setter for trustworthy AI (European Commission, 2024). Similarly, the **Cyber Resilience Act (2024)** introduced mandatory security requirements for digital products, strengthening resilience across the internal market (European Commission, 2024). Most recently, the **Cloud and AI Development Act**—opened for public consultation in April 2025—aims to accelerate the construction of European cloud infrastructures, potentially reshaping the competitive balance vis-à-vis dominant U.S. providers (European Commission, 2025).

Collectively, these initiatives illustrate how the EU leverages its regulatory capacity to exert normative influence internationally—a phenomenon described as the *Brussels Effect* (Bradford, 2023). In practice, this regulatory sovereignty enables the Union to shape global technology standards while remaining formally open to cooperation and trade. Scholars emphasize that this dual orientation—regulation as both a shield and a projection tool—represents a unique model of sovereignty, distinct from state-centric or developmental approaches (Farrell & Newman, 2024).

2.1.2 Defense Implications

Despite significant progress in digital governance, challenges persist regarding **European defense sovereignty**. Fragmentation across member states' procurement policies continues to undermine economies of scale, while reliance on non-EU suppliers for critical components creates structural vulnerabilities (Fiott, 2023). The **European Defence Fund (EDF)**, endowed with a budget of €8 billion for the period 2021–2027, represents a significant step towards collective capability development. However, analysts argue that this remains insufficient relative to the Union's sovereignty ambitions, especially when compared to U.S. and Chinese defense industrial investments (Simón, 2024).

The ongoing war in Ukraine has nonetheless catalyzed greater defense coordination. Joint procurement initiatives, the establishment of common stockpiles, and renewed standardization efforts across NATO and EU frameworks are progressively reducing fragmentation and reinforcing Europe's strategic autonomy (Simón, 2024). While technological sovereignty in digital domains advances primarily through regulation and industrial policy, defense sovereignty will depend on reconciling national preferences with collective action mechanisms capable of scaling investments and fostering interoperability.

2.2 United States: Technological Superiority as Strategic Imperative

The United States has undergone a profound recalibration of its technological policy landscape, moving away from a market-oriented paradigm toward an active industrial intervention model. This transformation is driven by the recognition that technological leadership is equivalent to strategic advantage in the twenty-first century (Mazzucato, 2021). The **CHIPS and Science Act of 2022**, allocating $53 billion for semiconductor research, development, and fabrication, represents the most visible expression of this shift. Production facilities in Arizona, Ohio, and Texas are expected to begin operations in 2024, symbolizing a new era of industrial policy centered on supply chain security and national resilience (U.S. Congress, 2022).

2.2.1 Strategic Pivots

Contemporary U.S. policy reflects three strategic pivots. First, there is a movement **from globalization to selective decoupling**, whereby Washington continues to uphold broad economic ties while imposing export controls on dual-use and advanced technologies. Restrictions on semiconductor manufacturing equipment and AI chips destined for China exemplify this calibrated approach (Council on Foreign Relations, 2023). Second, a shift **from private innovation to public–private fusion** is evident in the growing role of the federal government in directly shaping technology trajectories. Institutions such as the Defense Advanced Research Projects Agency (DARPA), the Advanced Research Projects Agency–Energy (ARPA-E), and the newly established ARPA-H for health technologies highlight the enduring model of mission-oriented innovation (Bonvillian & Van Atta, 2021). Third, U.S. strategy is reorienting **from unilateral leadership to coalition-building**, exemplified by the 2024 *U.S. International Cyberspace & Digital Policy Strategy*. This framework emphasizes building "open, secure, and interoperable" systems in partnership with allies such as France, Japan, South Korea, Sweden, and the United Kingdom, particularly in the context of 6G development and emerging digital standards (U.S. Department of State, 2024).

2.2.2 Security Integration

The **Pentagon's 2024 National Defense Industrial Strategy** consolidates the linkage between technological sovereignty and military superiority. Unlike earlier frameworks, this strategy explicitly situates industrial capacity and technological innovation as prerequisites for operational advantage (Brown & Daniels, 2024). Central initiatives include the accelerated integration of **artificial intelligence into command-and-control architectures**, enabling real-time data fusion and decision support; the development of **quantum computing programs** for cryptography and sensing, critical for secure communications and intelligence operations; advances in **hypersonic weapons** to preserve deterrence credibility against near-peer adversaries; and the expansion of **space-based capabilities** to guarantee resilient satellite communications and navigation systems (Scharre, 2023; Fiott, 2023; Sanz et al., 2024).

These efforts reflect the growing recognition that future conflicts will be shaped less by numerical force metrics than by **technological superiority**. The recalibration of U.S. industrial and defense strategies illustrates the embedding of technological sovereignty as a national security doctrine—positioning innovation ecosystems, industrial bases, and defense integration as mutually reinforcing pillars of American strategic autonomy (Farrell & Newman, 2024).

3.3 China: Comprehensive State-Led Transformation

3.3.1 China's Intensified Sovereignty Strategy

China's technological sovereignty strategy has intensified markedly in the aftermath of U.S. export controls and technology restrictions, which Beijing interprets as efforts to constrain its rise as a global power. In response, China has accelerated initiatives aimed at **indigenous innovation** and **self-reliance** across strategic sectors. The **14th Five-Year Plan (2021–2025)** identifies technological self-sufficiency as a national priority, with a particular focus on semiconductors, artificial intelligence, and quantum technologies (State Council of China, 2021). Complementing this, the so-called **"New Whole-Nation System"** (*xin juguo tizhi*) mobilizes state resources, universities, research institutes, and private enterprises to achieve breakthrough innovations in frontier domains (Wang & Feng, 2023).

3.3.2 Adaptive Strategies

Despite sustained U.S. export controls, Chinese firms have demonstrated notable resilience. In 2024, **Huawei** launched smartphones featuring advanced domestically produced semiconductors, signaling progress in overcoming barriers to access to Western technology (Lee, 2024). China's adaptive strategy combines four core mechanisms. First, the state is channeling **massive investments in R&D**, with targets to raise expenditures to over 3% of GDP by 2025, thereby placing China among the world's leaders in research intensity (OECD, 2023). Second, **talent recruitment programs** such as the *Thousand Talents Plan* continue to attract overseas expertise, facilitating knowledge transfer despite rising geopolitical frictions (Cao, 2022). Third, Beijing leverages **standards leadership** by embedding Chinese technical specifications into **Belt and Road Initiative (BRI) digital infrastructure projects**, thereby exporting its regulatory models to partner countries (Shen, 2023). Finally, the policy of **military–civil fusion** ensures that advances in commercial technology feed directly into defense applications, reinforcing the strategic synergy between civilian innovation and military modernization (Kania & Costello, 2018).

The scale of China's industrial mobilization is unprecedented. By 2024, China is projected to add more semiconductor manufacturing capacity than the rest of the world combined, producing an additional **one million wafers per month** relative to 2023 levels (Lee, 2024). This expansion demonstrates not only China's determination to reduce dependence on Western suppliers but also its capacity to leverage industrial planning for rapid scaling.

3.3.3 Global Implications

China's sovereignty model exerts growing influence on global technology governance through three principal mechanisms. First, **market leverage**: by conditioning access to its vast domestic market on compliance with Chinese standards and practices, Beijing is able to shape the behavior of foreign firms (Segal, 2020). Second, **standards proliferation**: through international organizations and bilateral agreements linked to the BRI, China actively promotes the diffusion of technical standards aligned with its regulatory preferences (Shen, 2023). Third, **alternative ecosystems**: by building parallel technological infrastructures—from payment platforms to cloud services and satellite systems—China offers an alternative to Western-dominated stacks, particularly attractive to developing countries seeking affordable and politically non-conditional digital infrastructure (Wang & Feng, 2023).

This approach challenges core assumptions of the liberal international order, which is predicated on open markets and universal standards. Instead, China advances a sovereignty model grounded in state-centric control, industrial self-reliance, and geopolitical assertiveness. At the same time, it provides a template for developing

economies, which may perceive in China's trajectory a viable alternative pathway to digital modernization without dependence on Western regulatory or financial frameworks (Lee, 2024; Wang & Feng, 2023).

3.4 Russia: Sovereignty Through Isolation

Russia's approach to sovereignty is explicitly securitized and rooted in a defensive posture vis-à-vis the West. The Sovereign Internet Law (2019) requires that all internet traffic in Russia be routed through state-controlled exchange points, allowing for the isolation of the RuNet from the global internet in case of perceived threats.

This reflects a doctrine of information sovereignty, emphasizing the state's right to regulate both the technical and content dimensions of the digital domain. For Moscow, digital sovereignty is inseparable from information control, including the ability to conduct disinformation campaigns abroad while insulating domestic information spaces from Western narratives (Pohle & Thiel, 2020).

Technological sovereignty is more problematic. Russia has long depended on Western technologies, from semiconductors to aircraft components. Sanctions following the annexation of Crimea (2014) and especially after the full-scale invasion of Ukraine (2022) have exacerbated these vulnerabilities. Moscow has responded with import substitution policies and increased reliance on Chinese technologies.

Russia's sovereignty strategy, dramatically accelerated by post-2022 sanctions, prioritizes survival over innovation. Unable to match Western technological capabilities, Russia pursues "defensive sovereignty" through isolation and control.

The "Sovereign RuNet" project progressed significantly, with successful isolation tests conducted in 2024, though full independence remains elusive (Stadnik, 2024; Epifanova, 2023).

From a defense perspective, digital and technological sovereignty are equated with autonomy in cyberwarfare, electronic warfare, and defense production under sanctions. Sovereignty thus serves as a survival strategy in conditions of isolation, emphasizing resilience rather than innovation.

3.5 India: Digital Public Infrastructure as Sovereignty Foundation

India's approach to sovereignty blends developmental objectives with strategic autonomy. The Indian model of state digital sovereignty is built around digital public infrastructures (DPIs), such as Aadhaar, the Unified Payments Interface (UPI), and DigiLocker, which enable both inclusion and control (Rajmohan, Singh, & Choudhury, 2025). India leverages these infrastructures not only to extend social services and expand financial inclusion but also to reduce dependency on global platforms and enhance national resilience. The emphasis on sovereign control over data, coupled with efforts to develop indigenous technological capacity, reflects a dual pursuit of inclusivity and strategic independence (Pant & Taneja, 2024).

India's comprehensive digital strategy illustrates this dual orientation. Facing growing cybersecurity challenges, including AI-enabled threats such as deepfakes and coordinated disinformation campaigns, India has launched measures that reinforce its sovereignty. These include the integration of Aadhaar into service delivery across sectors, the international expansion of UPI as a competitor to Western payment systems, mandatory data localization measures, and the development of indigenous 5G technologies to limit reliance on foreign suppliers. The publication of the Digital Threat Report 2024 further underscores India's sectoral approach to sovereignty, particularly in strengthening resilience in the banking, financial services, and insurance (BFSI) sector (Rajmohan et al., 2025).

India also practices strategic balancing through a policy of "multi-alignment," navigating between competing great powers. Technology partnerships with the United States, such as the Initiative on Critical and Emerging Technologies (iCET), coexist with selective engagement with Chinese technology in areas of necessity. At the same time, India asserts leadership in Global South digital governance forums, presenting itself as a voice for inclusive and equitable digital transformation. Indigenous capacities in space exploration, defense technologies, and cybersecurity reinforce this autonomy. By combining technological development with diplomatic flexibility, India maximizes its sovereignty while avoiding costly confrontations, thereby consolidating its role as a pivotal actor in the global digital order (Pant & Taneja, 2024; Rajagopalan, 2023).

This specific approach uniquely combines developmental objectives with strategic autonomy, leveraging digital public infrastructure (DPI) for both inclusion and control. India's model of state digital sovereignty emphasizes digital public infrastructures and strategic self-reliance.

India's comprehensive digital strategy illustrates the dual objective of promoting developmental inclusion while consolidating strategic autonomy. As of 2024, the country faces increasingly complex cybersecurity challenges, particularly those associated with artificial intelligence–enabled threats such as deepfakes and sophisticated manipulation of social media platforms (Gangi, 2025). The government's response has combined regulatory and technological measures aimed at strengthening sovereignty. Among the most significant actions are the expansion of Aadhaar integration into public service delivery systems, the internationalization of the Unified Payments Interface (UPI) as a challenge to the dominance of Western payment systems, and the imposition of data localization requirements designed to balance openness with sovereign control. Simultaneously, India has prioritized the development of indigenous 5G technology, thereby reducing its dependence on foreign suppliers and asserting its technological self-reliance. The publication of the **Digital Threat Report 2024** further demonstrates India's sectoral approach to sovereignty, highlighting targeted measures to reinforce cybersecurity resilience within the banking, financial services, and insurance sectors.

India also complements its internal digital strategy with a deliberate effort at strategic balancing through a policy of "multi-alignment." This foreign policy orientation allows India to maintain simultaneous partnerships with competing global powers while safeguarding its own autonomy. In the technological domain, this translates into deepening collaborations with the United States through initiatives such as the Initiative on Critical and Emerging Technologies (iCET), while continuing selective engagement with Chinese technology in areas deemed unavoidable. At the same time, India asserts leadership in Global South digital governance forums, using its developmental model of digital public infrastructure to position itself as a normative entrepreneur advocating inclusive and equitable governance of emerging technologies. Parallel to these efforts, India invests heavily in indigenous capacities in space exploration, defense technologies, and cybersecurity innovation. Through this strategy, India maximizes its strategic autonomy, leverages technological sovereignty as a tool for influence, and avoids costly confrontations in the polarized environment of global digital geopolitics (Pant & Taneja, 2024; Rajagopalan, 2023).

3.6 Japan: Trusted Connectivity and Resilient Networks

Japan's sovereignty strategy emphasizes reliability and trust rather than autarky, reflecting its long-standing preference for resilience within an interconnected order. A turning point occurred in 2024, when the National Parliament passed the landmark **Active Cyber Defense Law**, which signaled a decisive shift in the country's cybersecurity posture. This legislation, by granting the government greater authority to monitor and respond proactively to cyberattacks, institutionalizes a more assertive defense strategy that integrates sovereignty with national security imperatives.

The broader framework for Japan's approach to sovereignty had already been articulated in the **Economic Security Promotion Act of 2022**, which operationalizes sovereignty across four main pillars: strengthening supply chain resilience for critical materials, securing infrastructures essential to daily life, promoting technological development in strategic sectors, and protecting sensitive innovations through mechanisms such as patent non-disclosure. These pillars were reinforced in practice in February 2024, when Japan conducted its first large-scale cybersecurity exercise with Blue Pacific nations. This exercise, focused on responding to cyberattacks and defending critical infrastructure, underscored Tokyo's intention to develop practical capabilities while anchoring its leadership in regional security networks.

Alliance integration remains central to Japan's sovereignty strategy. In March 2024, Google established its first cyber defense center for the Asia-Pacific region in Tokyo, promoting advanced research on cyber threat mitigation and resilience. This development illustrates how Japan balances foreign partnerships with its domestic objectives. On one hand, Tokyo deepens joint technology development with the United States and other allies while exercising regional leadership in the setting of trusted technology standards. On the other, it invests in indigenous technological capabilities to avoid excessive dependencies, ensuring that sovereignty complements rather than undermines interoperability with allies. Japan also advances diplomatic initiatives under the banner of "Data Free Flow with Trust," positioning itself as a bridge between competing visions of the global digital order (Hemmings, 2024; Shiozawa, 2022).

3.7 Latin America: Developmental Sovereignty and Regional Cooperation

Latin America approaches digital and technological sovereignty primarily through the lenses of development, inclusion, and dependency reduction. Scholars and policymakers highlight the region's persistent vulnerability to technological dependency, as most digital infrastructures remain dominated by U.S.-based firms and critical technologies continue to be imported from abroad (OECD, 2020). This structural asymmetry has shaped sovereignty

debates, where the emphasis lies not on global power rivalry but on building the capacity to govern digital infrastructures in ways that promote socioeconomic development. Within this context, digital sovereignty is framed as both a regulatory and developmental project that seeks to reduce foreign dependency while strengthening local innovation ecosystems (Belli, 2023; Aguerre, 2024).

Debates around digital sovereignty in the region concentrate on data protection and connectivity. Brazil has advanced initiatives such as data localization requirements and national cloud strategies, aiming to ensure state authority over sensitive data and enhance security in the financial and government sectors (Aguerre, 2024). Mexico, in contrast, has focused on regulatory reforms to expand digital rights and constrain the dominance of global platforms, aligning its digital agenda with democratic and inclusive principles (Belli, 2023). Chile, meanwhile, has positioned itself as a leader in digital government services and infrastructure, experimenting with digital identities and open government platforms. Regional organizations such as the Inter-American Development Bank (IDB) and the OECD have supported these efforts by promoting cross-border cooperation on digital public goods and digital transformation agendas (OECD & IDB, 2023).

Technological sovereignty in Latin America is often framed as a process of capacity-building for innovation and resilience. Argentina has emphasized the development of defense-related technological autonomy, particularly in areas such as aerospace and nuclear technologies, where national security concerns intersect with industrial development goals. Brazil, with a long history of indigenous aerospace and satellite projects, continues to invest in domestic technological capabilities as part of its strategic vision. Chile has leveraged its digital governance expertise to attract investment and consolidate its position as a hub for regional digital innovation. Yet, despite these national strategies, the region continues to face structural limitations, such as low R&D spending, limited venture capital, and brain drain, which weaken long-term technological sovereignty (OECD & IDB, 2023).

For defense and security, Latin American states tend to view sovereignty less in terms of global great-power competition and more as a tool for ensuring autonomy in crisis response, resilience to cybercrime, and advancing regional integration. Sovereignty thus operates as a developmental instrument that also generates security benefits in areas such as critical infrastructure protection, countering cyberattacks, and building regional defense cooperation (Rodríguez et al., 2023) As cybercrime and digital espionage intensify in the region, governments are increasingly aware that sovereignty has both economic and security dimensions, even if framed within developmental logics (Epifanova, 2023; Fiott, 2023).

4. Comparative Analysis: Models, Metrics, and Trajectories

The comparative analysis of digital and technological sovereignty across leading states and regions reveals both convergence and divergence in policy objectives, instruments, and security implications. On the one hand, there is a near-universal acknowledgment that control over digital infrastructures and technological capacities has become indispensable for national security, economic resilience, and political autonomy. On the other hand, the normative foundations, institutional approaches, and practical strategies adopted by different actors vary widely, reflecting distinct political cultures, developmental trajectories, and security imperatives.

4.1 Convergent vision is not limited to technological evolution

A first point of convergence lies in the recognition that digital and technological sovereignty are no longer optional ambitions but strategic necessities. The increasing weaponization of interdependence (Farrell & Newman, 2019), whereby states exploit chokepoints in global supply chains and digital ecosystems for coercive leverage, has made vulnerability unacceptable in the eyes of policymakers. This dynamic has been reinforced by the geopoliticization of emerging technologies such as semiconductors, artificial intelligence, and 5G networks, all of which have become arenas of competition between great powers (Mueller, 2020; Sanz et al., 2024: Gangi, 2025).). The rise of sophisticated cyberattacks and disinformation campaigns further illustrates how reliance on external providers and global platforms can expose states to strategic risks. Even in regions traditionally marginalized in technological competition, such as Latin America, sovereignty is increasingly framed as a defense against dependency and a means of ensuring resilience in the face of external shocks (OECD & IDB, 2023).

Despite these shared concerns, the normative foundations of sovereignty diverge sharply. The European Union (EU) has articulated the concept in terms of “open strategic autonomy,” seeking to balance interdependence with regulatory capacity. Here, sovereignty is understood less as insulation from global flows and more as the ability to shape them in accordance with European values such as privacy, data protection, and ethical artificial intelligence (European Commission, 2021; Floridi, 2020). In contrast, the United States avoids the sovereignty terminology but

pursues a functionally equivalent agenda by framing sovereignty in terms of technological leadership, innovation capacity, and industrial resilience. Its policy discourse prioritizes superiority over competitors, particularly China, and links technological dominance to national defense and deterrence (White House, 2021). China, by contrast, advances a doctrine of "cyberspace sovereignty" (wangluo zhuquan), rooted in the principle of supreme state authority over digital domains. For Beijing, sovereignty entails comprehensive control of internet infrastructures, data flows, and technological standards, reinforced through extensive legislation and state-led innovation strategies (Standing Committee of NPC, 2021; State Council, 2023). Russia's approach is even more securitized: sovereignty is equated with the capacity to control information space and insulate the domestic internet (RuNet) from Western influence (Cruz % Liz, 2019). This reflects a defensive posture under conditions of isolation and sanctions, in which survival takes precedence over innovation (Pohle & Thiel, 2020).

Other regions and states pursue sovereignty with different emphases. In Latin America, sovereignty discourses revolve around development and inclusion. Governments and regional organizations stress the need to reduce dependency on foreign platforms and infrastructures, while expanding access to connectivity and protecting citizens' digital rights (OECD, 2020). India blends developmental and security imperatives by building extensive digital public infrastructures (DPIs) such as Aadhaar and the Unified Payments Interface (UPI). These systems both extend state control over digital ecosystems and foster inclusive growth, embodying a hybrid model of self-reliance (Atmanirbhar Bharat) and strategic openness to alliances (Rajmohan et al., 2025). Japan, meanwhile, articulates sovereignty around the notion of "trusted connectivity." Through initiatives such as the Data Free Flow with Trust (DFFT), Japan seeks to reconcile openness to global flows with resilience in supply chains and infrastructures, embedding sovereignty in international norms of transparency and reliability (Shiozawa, 2022). These contrasting perspectives confirm that sovereignty is not a universal or monolithic concept but one mediated by historical experiences, political cultures, and normative priorities.

4.2 Objects of sovereignty are in permanent evolution

The objects of sovereignty also vary across cases. In the EU, data protection and semiconductors have emerged as core objects of control, reflecting both regulatory priorities and industrial vulnerabilities (European Chips Act, 2023). The United States focuses primarily on semiconductors, artificial intelligence, and defense-critical technologies, perceiving them as essential to maintaining military superiority (DARPA; DIU). China pursues a comprehensive agenda that encompasses telecommunications, AI, quantum computing, and standard-setting, aiming at systemic autonomy and eventual global leadership (Made in China 2025; China Standards 2035). Russia's objects of sovereignty are narrower, constrained by sanctions and industrial limitations, with emphasis placed on internet infrastructures and defense technologies. Latin American countries prioritize connectivity, cloud infrastructures, and localized software ecosystems, linking sovereignty to socio-economic development (OECD & IDB, 2023). India emphasizes both digital ID systems and semiconductors, reflecting its dual concern with governance and industrial capacity (Rajmohan et al., 2025). Japan, finally, prioritizes supply chains, semiconductors, and data governance, reflecting its role as a manufacturing hub embedded in a volatile regional security environment (Shiozawa, 2022).

Policy instruments also diverge significantly. The EU relies heavily on regulation, exemplified by the General Data Protection Regulation (GDPR), the Digital Compass, and sectoral strategies such as the Chips Act. These are complemented by defense cooperation mechanisms such as the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO). The United States employs industrial subsidies, executive orders, and public–private innovation ecosystems, exemplified by DARPA and the Defense Innovation Unit. China combines legislation with industrial strategies such as Made in China 2025 and China Standards 2035, reinforced by the civil–military fusion doctrine. Russia employs legal frameworks for internet control and policies of import substitution, though its capacity to develop alternatives remains limited. Latin America employs softer instruments such as regional cooperation initiatives, public cloud programs, and data protection frameworks. India leverages national programs like Digital India, Semicon India, and Atmanirbhar Bharat, alongside bans on foreign digital platforms deemed hostile. Japan's toolkit includes the Economic Security Promotion Act, supply chain oversight, and alliance frameworks, complemented by global initiatives such as DFFT. These variations highlight that sovereignty can be pursued through regulatory, industrial, authoritarian, or cooperative means, depending on the political and institutional context.

4.3 Sovereignty is measurable

Metrics for evaluating sovereignty similarly differ. In the EU, sovereignty is measured through indicators such as the share of global chip production, compliance with GDPR, and participation in PESCO projects (European Parliament, 2025). In the United States, the focus lies on levels of domestic semiconductor production, R&D spending,

and the depth of public–private partnerships. In China, the key metrics include the share of global patents in AI and 5G, compliance with data localization requirements, and global adoption of Chinese technological standards. Russia measures sovereignty through its capacity to isolate the RuNet and sustain defense production under sanctions. Latin America evaluates sovereignty in terms of connectivity access, local software development, and digital inclusion (OECD & IDB, 2023). India's benchmarks include the usage of DPIs, domestic chip production, and the growth of startups in critical sectors (Rajmohan et al., 2025). Japan focuses on diversification of supply chains and adoption of trusted standards (Shiozawa, 2022). These differences underscore that sovereignty is operationalized not only in diverse ways but also through heterogeneous criteria of success.

Nonetheless, each region faces significant challenges and contradictions in its pursuit of sovereignty. The EU struggles with fragmentation between member states and continued reliance on foreign platforms and hardware (European Parliament, 2025). The United States faces internal contradictions between its ideological preference for free markets and its increasing reliance on industrial policy. China risks isolation and innovation slowdown due to restrictions on openness and mounting sanctions. Russia's sovereignty remains more aspirational than real, given its structural dependencies and technological backwardness. Latin America continues to grapple with a persistent digital divide, underinvestment in research and development, and limited bargaining power in global value chains. India faces the tension of reconciling openness to foreign investment and partnerships with its drive for self-reliance. Japan's vulnerabilities include heavy dependence on energy imports and geopolitical pressures stemming from its proximity to China and North Korea. These challenges illustrate the paradox of sovereignty in the digital era: while full autonomy is unattainable in a globalized ecosystem, dependency is increasingly perceived as a strategic liability.

4.4 National and regional security implications must be considered

The implications for security and defense are far-reaching. Semiconductors have become a central battlefield, with the United States, EU, China, Japan, and India all investing heavily in domestic production capacity. Cybersecurity and cyberwarfare are transversal concerns: while Russia and China emphasize control and offensive capacities, the EU and United States focus on resilience and defense, and Latin America stresses capacity-building against cybercrime. Military supply chains are increasingly securitized, particularly in U.S. and Japanese strategies, as well as in China's civil–military fusion agenda. Standard-setting has become a domain of strategic competition, with China and the EU vying to shape international rules, while Japan and India align with U.S.-led coalitions. In sum, digital and technological sovereignty are no longer limited to economic or developmental debates but have become central to defense planning, alliance politics, and deterrence strategies.

A final synthesis suggests the emergence of three distinct models of sovereignty. The normative-regulatory model, exemplified by the EU and Japan, conceives sovereignty as the capacity to shape global norms and ensure trusted, rights-based governance. The industrial-security model, pursued by the United States and India, emphasizes innovation, industrial capacity, and integration with defense strategies. The authoritarian-control model, advanced by China and Russia, conceives sovereignty as state authority, self-sufficiency, and securitization of digital ecosystems. Latin America, while less cohesive, represents a hybrid developmental model in which sovereignty is framed as resilience and inclusion rather than dominance. These models confirm that sovereignty is plural and contested in the digital age, reflecting the interplay of national security imperatives, political cultures, and global competition. Yet, despite these differences, their coexistence generates new arenas of rivalry and cooperation, making sovereignty itself a central site in the ongoing reconfiguration of the international order.

4.5 Convergent Trends Across Regions

Despite diverse approaches, several convergent trends emerge with specific:

- Universal Securitization: All examined states now frame digital-technological capabilities as national security imperatives. India, Indonesia, Japan, and South Korea are independently and jointly working to strengthen cybersecurity and cyber resilience, reflecting regional coordination alongside national efforts.
- Industrial Policy Renaissance: Market-oriented economies embrace state intervention, with industrial policy returning as legitimate tool for sovereignty. Even traditionally liberal economies recognize market failures in securing strategic technologies.
- Standards Competition: Technical standards become geopolitical battlegrounds, with competing visions of internet governance, AI ethics, and data protection reflecting deeper normative conflicts.
- Supply Chain Securitization: The semiconductor shortage revealed universal vulnerability, spurring efforts to "reshore," "nearshore," or "friendshore" critical production.

5. Security and Defense Implications

The growing emphasis on digital and technological sovereignty constitutes one of the most significant transformations in international security and defense strategy since the end of the Cold War. While globalization was once celebrated for its potential to spread prosperity and reduce conflict, the weaponization of interdependence has turned technological linkages into sources of vulnerability. As states recognize the risks of dependence on foreign infrastructures, supply chains, and standards, they increasingly frame sovereignty not as an abstract principle but as a practical condition for security, autonomy, and resilience. This section explores the implications of sovereignty discourses for global security, examining their impact on power competition, alliance politics, military planning, and the prospects for cooperation or fragmentation in the digital age.

5.1 Sovereignty and Strategic Autonomy

The pursuit of sovereignty has reshaped the notion of strategic autonomy; a concept long associated with defense independence. In the European Union, strategic autonomy has expanded from military capabilities to digital infrastructures, semiconductors, and data governance (European Commission, 2021). The idea is that without control over digital backbones, defense systems remain vulnerable to external interference. Similarly, in the United States, sovereignty discourse manifests as a push for "technological leadership" in fields like artificial intelligence and microelectronics, linking industrial competitiveness directly to deterrence and military superiority (White House, 2021). For China and Russia, sovereignty is framed as a prerequisite for resisting external coercion and ensuring regime survival. In all cases, sovereignty becomes synonymous with security, blurring the traditional distinction between economic and defense domains (Payá & Luque , 2021).

This redefinition also reflects a deeper structural change: technology has become both the means and the object of geopolitical rivalry. Control over semiconductors, cloud services, and communication standards is no longer just a matter of economic competition but a determinant of military effectiveness. As a result, sovereignty initiatives increasingly aim to fuse industrial and defense strategies. China's doctrine of civil–military fusion exemplifies this trend by integrating private technological innovation directly into defense planning (State Council, 2023). The United States has responded with public–private initiatives through DARPA and the Defense Innovation Unit, emphasizing innovation ecosystems as national security assets. Europe, though more hesitant, has begun to embed technological resilience into its defense policies through PESCO and the European Defence Fund. This fusion underscores the centrality of sovereignty for strategic autonomy in the twenty-first century.

5.2 Military Supply Chains and Defense Industrial Bases

Military power increasingly depends on secure and resilient supply chains. The COVID-19 pandemic and subsequent disruptions in global trade highlighted the vulnerability of defense industrial bases to external shocks. The semiconductor shortage, in particular, revealed that even the most advanced militaries depend on fragile supply lines concentrated in East Asia. This has prompted a global rush to "re-shore" or "friend-shore" critical production. The United States' CHIPS and Science Act of 2022 exemplifies how sovereignty concerns translate into industrial subsidies aimed at securing military supply chains. Japan and India have launched similar initiatives, seeking both economic and defense dividends (Shiozawa, 2022; Rajmohan et al., 2025).

For Russia, sanctions following the 2022 invasion of Ukraine have made sovereignty synonymous with survival, as the country struggles to sustain its defense production without access to Western components. China, meanwhile, views U.S.-led restrictions on semiconductor exports as an existential threat to its sovereignty, spurring massive investments in domestic manufacturing. The EU has pursued a middle path, combining industrial policy with alliances, as seen in its efforts to diversify suppliers while strengthening domestic capacity. Across these cases, military supply chains emerge as both vulnerabilities and strategic tools, illustrating how sovereignty discourses reshape defense industrial policy.

5.3 Cybersecurity, Cyberwarfare, and Sovereignty

The cyber domain is a key arena where digital sovereignty directly intersects with defense. For authoritarian regimes such as China and Russia, sovereignty is equated with the ability to control cyberspace and project offensive capabilities. Russia's experiments with the "sovereign RuNet" and China's comprehensive data localization laws illustrate a securitized vision of cyberspace in which control is paramount (Standing Committee of NPC, 2021). For democratic states, sovereignty is often framed in terms of resilience, emphasizing cybersecurity, protection of critical infrastructures, and safeguarding of democratic processes from disinformation campaigns (Pohle & Thiel, 2020).

The divergence in approaches reflects deeper normative differences. While China and Russia justify cyber-sovereignty as an extension of state authority, the EU and Japan emphasize values of trust and accountability. The United States, meanwhile, adopts a more offensive posture, linking sovereignty to deterrence in cyberspace and maintaining the capacity to conduct retaliatory operations against adversaries. Latin American states, with more limited capabilities, frame sovereignty in terms of protection from cybercrime and transnational threats, stressing regional cooperation (Rodríguez et al., 2023). Thus, sovereignty in cyberspace both deepens geopolitical rivalries and creates new inequalities in capacity-building, with security consequences for states across the spectrum (Martino et al., 2024).

5.4 Standards, Alliances, and Global Governance

Technological standards are an emerging battleground of sovereignty. China's China Standards 2035 plan explicitly seeks to shape international norms and technical standards, leveraging its domestic market size to gain influence (State Council, 2023). The EU responds with its normative-regulatory power, advancing global frameworks for data protection and AI ethics (Floridi, 2020). The United States prioritizes coalitions such as the Quad and G7 to counter Chinese influence in 5G and semiconductor standards. Japan's concept of "trusted connectivity" and India's leadership in digital public infrastructures both contribute to coalitional approaches that align with U.S. strategies while maintaining elements of autonomy (Shiozawa, 2022; Rajmohan et al., 2025).

The contest over standards illustrates that sovereignty is not purely inward-looking but also externally oriented: by shaping global rules, states can extend their sovereignty beyond borders. However, this also fragments global governance, creating rival ecosystems that undermine the universality of the internet and reduce interoperability. For defense alliances such as NATO, this fragmentation poses operational challenges, as interoperability of communication systems and data sharing are essential for joint operations. Sovereignty discourses thus complicate alliance management, forcing states to reconcile national autonomy with collective defense needs.

5.5 The Paradox of Interdependence

A persistent paradox runs through all sovereignty strategies: while autonomy is the goal, interdependence remains inescapable. No state, not even the United States or China, can achieve complete self-sufficiency in all technological domains. Supply chains for advanced chips, rare earth minerals, and AI development remain global by nature. Attempts to decouple risk not only inefficiency but also destabilization of the global economy. The challenge, therefore, is to balance sovereignty with selective interdependence. The EU's concept of "open strategic autonomy" reflects this balance, as does Japan's emphasis on trusted networks. India's dual strategy of Atmanirbhar Bharat and international partnerships also illustrates the search for equilibrium. Even China, despite its rhetoric of self-reliance, continues to rely on global markets for energy, raw materials, and certain advanced components. This paradox complicates the security landscape: while sovereignty strategies aim to reduce vulnerability, they simultaneously create new dependencies, shifting rather than eliminating risks.

5.6 Sovereignty as a Driver of Power Competition

Finally, sovereignty has become a driver of great-power rivalry. The U.S.–China competition is structured around sovereignty discourses, with both sides framing technological dominance as essential to security. Russia, though less technologically competitive, uses sovereignty rhetoric to justify autarky and resistance to Western influence. The EU seeks to carve out a middle ground, leveraging sovereignty to enhance its global role without fully decoupling from either camp. India and Japan position themselves as pivotal players, using sovereignty strategies to strengthen alliances while preserving autonomy. Latin America remains on the periphery but increasingly recognizes sovereignty as a bargaining chip in its relations with larger powers.

This competition has significant security implications. It risks fragmenting the global digital order into rival blocs, complicating cooperation on transnational challenges such as cybercrime, climate change, and pandemic response. It also intensifies the arms race in emerging technologies, as states invest heavily in AI, quantum computing, and cybersecurity for strategic advantage (Martino et al., 2024). The militarization of technological competition raises the prospect of new forms of conflict, where sovereignty claims serve as justification for offensive operations or coercive measures. In this sense, sovereignty is not only a defensive posture but also a catalyst of rivalry, embedding technological competition within the broader dynamics of international security (Martino, 2023).

5.7 Synthesis

Taken together, these dynamics suggest that digital and technological sovereignty are transforming global security in three main ways. First, they redefine strategic autonomy, making control of infrastructures and technologies as important as military hardware. Second, they reconfigure alliances and governance, as states seek to reconcile national autonomy with collective defense and global interoperability. Third, they intensify power competition, embedding technological rivalry within defense strategies and fueling geopolitical polarization. The pursuit of sovereignty thus emerges as both a response to insecurity and a source of new insecurities. For security and defense communities, this duality constitutes both an opportunity and a challenge: sovereignty can enhance resilience and autonomy, but it can also deepen fragmentation and rivalry. The future of international security will therefore hinge on whether sovereignty discourses evolve into cooperative frameworks or harden into confrontational blocs.

6. Conclusion

Digital and technological sovereignty has emerged as a defining feature of contemporary international security, fundamentally reshaping state behavior, alliance dynamics, and strategic competition. This comprehensive analysis reveals that while states universally recognize sovereignty's importance for strategic autonomy, profound differences persist in conceptualization and implementation.

The different perspectives reflect deeper disagreements about the relationship between state authority, market forces, and individual rights in the digital age. These differences are not merely theoretical but translate into concrete policy choices with significant security implications. Digital sovereignty requires states to regulate and control digital services and infrastructures, ensuring citizen rights protection and national interest safeguarding.

For defense communities, sovereignty presents both opportunities and challenges. On one hand, sovereign capabilities enhance resilience, reduce vulnerabilities, and provide strategic advantages. On the other hand, sovereignty pursuit risks fragmenting alliances, reducing interoperability, and triggering destabilizing competition. The challenge lies in developing sovereignty strategies that enhance security without undermining cooperation.

Looking forward, several trends will shape sovereignty's evolution:

- Technological Acceleration: Emerging technologies like quantum computing, synthetic biology, and artificial general intelligence will create new sovereignty imperatives while potentially disrupting existing strategies.
- Geopolitical Realignment: The crystallization of technological blocs appears increasingly likely, with states forced to choose between competing ecosystems or attempt costly neutrality.
- Normative Competition: The contest between different sovereignty models reflects deeper struggles over the future of global governance, with implications extending beyond technology to fundamental questions about political order.
- Economic Constraints: The massive investments required for sovereignty will strain budgets and force difficult trade-offs between autonomy and other priorities.

The twenty-first century has witnessed the emergence of digital and technological sovereignty as central pillars of national security, economic policy, and global power competition. What was once perceived as a technical or economic issue has now become a matter of strategic survival. States and regions around the world—whether the European Union, the United States, China, Russia, India, Japan, or Latin America—have reframed sovereignty as the ability to control critical infrastructures, shape digital ecosystems, and reduce vulnerability to coercion. This article has argued that while sovereignty discourses share a common concern with resilience and autonomy, they differ profoundly in their normative orientations, instruments, and geopolitical consequences.

At the conceptual level, two distinctions are critical. Digital sovereignty refers primarily to control over data, digital infrastructures, and cyberspace governance, while technological sovereignty encompasses mastery of physical and emerging technologies such as semiconductors, artificial intelligence, and quantum computing (Martino, 2023; Sanz et al., 2024). Both dimensions overlap but are not identical; together they constitute the foundations of strategic autonomy in the digital age. By disentangling these dimensions, it becomes possible to understand how different states prioritize specific domains and why sovereignty discourses vary across contexts (Gangi, 2025).

From a comparative perspective, three broad models of sovereignty can be identified. The normative-regulatory model, exemplified by the European Union and Japan, emphasizes the ability to set rules, standards, and values that govern the digital order. Here, sovereignty is not isolationist but outward-looking, seeking to shape global flows in ways consistent with democratic principles, privacy, and trusted connectivity. The industrial-security model, pursued by the United States and India, prioritizes innovation capacity, industrial competitiveness, and integration of

technological advances into defense planning. This model is less concerned with global norms than with maintaining superiority over rivals and ensuring secure military supply chains. The authoritarian-control model, advanced by China and Russia, equates sovereignty with centralized state authority over digital and technological infrastructures, embedding control into strategies of regime survival and geopolitical confrontation. Latin America, though less coherent, presents a developmental variant that frames sovereignty as resilience against dependency and as a tool for inclusive digital transformation.

These sovereignty models are not static but interact dynamically, shaping the evolving landscape of global security. The U.S.–China rivalry, for instance, pits industrial-security against authoritarian-control models, fueling an arms race in emerging technologies and fragmenting global supply chains. The EU's normative-regulatory approach seeks to mitigate this polarization by offering a third path, though it struggles with internal divisions and persistent dependencies. India and Japan occupy pivotal positions, leveraging sovereignty discourses to strengthen alliances while preserving elements of autonomy. Latin America, while peripheral in the global contest, illustrates how sovereignty narratives can empower weaker actors to negotiate better terms of integration into the digital economy.

Sovereignty strategies redefine the concept of strategic autonomy, expanding it beyond traditional military independence to include technological infrastructures, data governance, and innovation ecosystems. They also reconfigure defense industrial policies, as states seek to secure supply chains for semiconductors, rare earth minerals, and dual-use technologies. Moreover, sovereignty discourses shape alliance politics: NATO and other defense partnerships must now reconcile national drives for autonomy with the operational need for interoperability. In cyberspace, sovereignty fuels both resilience and confrontation, as states seek to protect critical infrastructures while simultaneously developing offensive capabilities (Martino et al., 2024). Yet the pursuit of sovereignty is fraught with contradictions. The paradox of interdependence remains unresolved: no state can achieve full technological self-sufficiency, and attempts at decoupling risk inefficiency, economic fragmentation, and even greater vulnerability. Sovereignty thus emerges as a relative and contested condition—an ongoing negotiation between autonomy and openness, between national control and global interconnection. This paradox generates tensions within states, as industrial policy collides with market logics, and across borders, as sovereignty claims fragment global governance into rival blocs.

Looking ahead, sovereignty is likely to become an enduring feature of international security debates. In the short term, competition will intensify around semiconductors, AI, quantum computing, and cybersecurity, with sovereignty discourses justifying protectionist policies and heavy investments in defense-related technologies (Martino, 2023). In the medium term, the contest over standards will shape the digital order, as competing models of sovereignty seek to institutionalize their principles in global governance structures. In the long term, the very nature of sovereignty may evolve, as technological change blurs distinctions between domestic and international, civilian and military, economic and security domains.

For scholars and practitioners of security and defense, three priorities stand out. First, it is essential to analyze sovereignty not as a uniform doctrine but as a plural and evolving set of strategies shaped by historical experiences, political cultures, and security imperatives (Martino et al., 2024; Payá et al., 2018)). Second, greater attention must be paid to the interaction between sovereignty and alliances, as the pursuit of autonomy may either undermine or reinforce collective defense structures. Third, research must explore pathways for reconciling sovereignty with global cooperation, especially on transnational challenges such as cybercrime, climate change, and digital inequality. Without such reconciliation, sovereignty risks becoming a source of fragmentation and conflict rather than resilience and security (Rodríguez et al., 2023; Martino, 2023).

In conclusion, digital and technological sovereignty are not passing trends but structural features of the emerging international order. They reflect both the vulnerabilities of globalization and the imperatives of security in a world where technology is the ultimate arena of power competition. While sovereignty promises resilience, autonomy, and strategic control, it also generates new insecurities, rivalries, and contradictions. Whether sovereignty evolves into a framework for cooperative resilience or a justification for geopolitical confrontation will determine the trajectory of international security in the decades to come. For defense communities and policymakers, engaging critically with sovereignty is therefore not only an intellectual necessity but also a strategic imperative (Luque et al., 2023; Martino, 2024).

States that successfully navigate the tension between autonomy and interdependence while maintaining innovative capacity and alliance cohesion will shape the emerging international order. Those that fail risk strategic irrelevance or subordination in hierarchical technology relationships.

For scholars and practitioners, the sovereignty challenge demands new conceptual frameworks, policy instruments, and strategic doctrines. Traditional approaches based on territorial sovereignty and market integration prove inadequate for digital realities. Instead, we need adaptive strategies recognizing sovereignty as an ongoing process rather than fixed condition—strategies that pursue resilience without autarky, autonomy without isolation, and security without fragmentation.

Ultimately, the sovereignty question reflects fundamental choices about the kind of international order we wish to create. Will sovereignty discourse produce a fragmented world of technological blocs and digital borders? Or can we develop frameworks reconciling legitimate sovereignty concerns with the benefits of interconnection and cooperation? The answer will determine not only the trajectory of technological development but also the prospects for peace and prosperity in the twenty-first century.

The path forward requires pragmatic recognition that absolute sovereignty is neither achievable nor desirable in an interconnected world. Instead, states must pursue "sufficient sovereignty"—maintaining control over truly critical capabilities while accepting interdependence elsewhere. This necessitates careful assessment of vulnerabilities, strategic prioritization of sovereignty investments, and creative diplomacy to build trusted networks that enhance collective resilience without sacrificing essential autonomy.

As this analysis demonstrates, digital and technological sovereignty represents not a return to autarkic nationalism but an evolution toward more sophisticated understandings of power, security, and autonomy in the digital age. The states and alliances that best navigate these complexities—balancing sovereignty with cooperation, autonomy with efficiency, and security with innovation—will define the strategic landscape for decades to come.

References

1. Aguerre, C. (2024). Digital sovereignty in Latin America: Between development aspirations and geopolitical pressures. *Telecommunications Policy, 48*(2), 102–118. https://doi.org/10.1016/j.telpol.2024.102718
2. Belli, L. (2023). Data sovereignty and digital development: The Latin American path. *Internet Policy Review, 12*(1), 1–22. https://doi.org/10.14763/2023.1.1681
3. Bendiek, A., & Stürzer, I. (2023). The EU's digital sovereignty: From regulatory power to digital industrial policy. *Journal of European Public Policy, 30*(4), 721–742. https://doi.org/10.1080/13501763.2023.2189456
4. Bonvillian, W. B., & Van Atta, R. (2021). *ARPA-E: Innovation, climate change, and national energy policy*. Routledge.
5. Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press. https://doi.org/10.1093/oso/9780197649268.001.0001
6. Brown, M., & Daniels, K. (2024). The role of emerging technologies in U.S. defense strategy. *Strategic Studies Quarterly, 18*(1), 45–67.
7. Cao, C. (2022). *China's pursuit of talent: Incentives and risks of the Thousand Talents Plan*. Routledge.
8. Cruz Beltrán, J.L & Liz Rivas, L. (2019). *El perfil del ciberterrorista: la utilización de medios informáticos con fines terroristas*, CIVITAS, pp. 159-173. https://doi.org/10.5281/zenodo.14562806
9. Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society, 21*(10), 2305–2321. https://doi.org/10.1177/1461444819865984
10. Couture, S., & Toupin, S. (2024). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society, 26*(3), 1456–1478. https://doi.org/10.1177/14614448231189012
11. Council on Foreign Relations. (2023). *U.S. export controls and the China tech rivalry*. https://www.cfr.org
12. Delgado Morán, J. J., Payá Santos, C. A., Sanz González, R. (2023). China's Borderless Expansionism. Could Be a Threat to International Security?. *Advanced Sciences and Technologies for Security Applications.* Springer, Cham. https://doi.org/10.1007/978-3-031-28336-9_5D
13. Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. *Research Policy, 52*(6), Article 104765. https://doi.org/10.1016/j.respol.2023.104765
14. Epifanova, A. (2023). Russia's digital sovereignty: Progress, isolation, and implications. *Post-Soviet Affairs, 39*(4), 312–329. https://doi.org/10.1080/1060586X.2023.2234567
15. European Commission. (2021). *2030 Digital Compass: The European way for the digital decade*. Publications Office of the EU. https://digital-strategy.ec.europa.eu/en/library/2030-digital-compass-european-way-digital-decade
16. European Commission. (2023). *The European Chips Act*. Publications Office of the EU. https://digital-strategy.ec.europa.eu/en/library/european-chips-act
17. European Commission. (2024a). *Artificial Intelligence Act*. Publications Office of the EU. https://artificialintelligenceact.eu
18. European Commission. (2024b). *Cyber Resilience Act*. Publications Office of the EU. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
19. European Commission. (2024c). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Publications Office of the EU. https://digital-strategy.ec.europa.eu/en/library/data-act

20. European Commission. (2025). *State of the Digital Decade 2025: Progress on digital transformation, security and technological sovereignty*. Publications Office of the EU.
21. European Parliament. (2025a). *Report on European technological sovereignty and digital infrastructure (A10-0107/2025)*. Directorate-General for External Policies.
22. European Parliament. (2025b). *Strategic autonomy and the EU's security agenda*. Directorate-General for External Policies.
23. Farrell, H., & Newman, A. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351
24. Farrell, H., & Newman, A. (2024). The new economic statecraft: How geoeconomics is reshaping great power competition. *International Security, 48*(4), 89–124. https://doi.org/10.1162/isec_a_00478
25. Fiott, D. (2023). The EU's strategic autonomy trap: Defence industrial policy and the war in Ukraine. *Journal of Common Market Studies, 61*(5), 1234–1250. https://doi.org/10.1111/jcms.13456
26. Fiott, D. (2023). *Strategic autonomy and European defence: Lessons from Ukraine*. European Union Institute for Security Studies. https://www.iss.europa.eu
27. Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6
28. Floridi, L. (2023). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press. https://doi.org/10.1093/oso/9780198883098.001.0001
29. Gangi Guillén, G. K. (2025). Derechos humanos y derecho penal en la era de la inteligencia artificial: retos y propuestas. *Cuadernos de RES PUBLICA en derecho y criminología*, https://doi.org/10.46661/respublica.11635
30. Hemmings, J. (2024). Japan's economic security strategy: Balancing openness and resilience. *International Affairs, 100*(2), 567–585. https://doi.org/10.1093/ia/iiae024
31. Kania, E., & Costello, J. (2018). *China's military-civil fusion strategy: Policy, practice, and implications for the United States*. Center for a New American Security.
32. Lee, K. (2024). China's innovation drive in the semiconductor and quantum industries. *Journal of Contemporary China, 33*(137), 455–472. https://doi.org/10.1080/10670564.2024.2314567
33. Luque Juárez, J. M., Payá Santos, C. A., & Arenas Morales, F. (2023). Contexto de las políticas de seguridad ciudadana. *Cuadernos de RES PUBLICA en derecho y criminología*, (2), 69–82. https://doi.org/10.46661/respublica.8293
34. March, S., & Schieferdecker, I. (2024). Rethinking technological sovereignty: Frameworks for resilient innovation ecosystems. *Journal of Technology Transfer, 49*(2), 145–168. https://doi.org/10.1007/s10961-023-09999-1
35. MARTINO, Luigi. (2024). Cybersecurity in Italy. Governance, Policies and Ecosystem. Springer Nature. https://doi.org/10.1007/978-3-031-64396-5
36. Martino, L. (2023). La guerra nel XXI secolo: la dimensione cyber e il conflitto russo-ucraino. In: *La guerra tiepida: Il conflitto ucraino e il futuro dei rapporti tra Russia e Occidente*. Rome: Luiss University Press.
37. Martino, L. (2024). International Law, State Sovereignty and Competition in the Digital Age. *Rivista di filosofia del diritto internazionale e della politica globale*, Vol. 21, Nº. 2, 2024. https://dialnet.unirioja.es/descarga/articulo/10098952.pdf
38. Martino, L; Paya Santos, C. A. & Delgado Morán, J, J. (2024). Thus,do they all: APTs as instruments of State-Sponsored cyber operations. *Eksploriump*. V. 45 No. 1s, 27-50. https://doi.org/10.52783/eksplorium.145
39. Mazurier, P, A., Delgado Morán, J, J., & Paya Santos, C, A. (2019). Gobernanza constructivista de la internet. *Teoría y Praxis*, 17(34), 107-130. https://doi.org/10.5377/typ.v1i34.14823
40. Mazzucato, M. (2021). *Mission economy: A moonshot guide to changing capitalism*. Penguin.
41. Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review, 22*(4), 779–801. https://doi.org/10.1093/isr/viz040
42. OECD. (2020). *Latin American economic outlook 2020: Digital transformation for building back better*. OECD Publishing. https://doi.org/10.1787/20725161
43. OECD. (2023). *Main Science and Technology Indicators 2023*. OECD Publishing. https://doi.org/10.1787/msti-v2023-1-en
44. OECD, & Inter-American Development Bank. (2023). *Latin American digital transformation report 2023*. OECD Publishing.
45. Pant, H. V., & Taneja, K. (2024). India's sovereignty and digital public infrastructures. *India Review, 23*(2), 210–228. https://doi.org/10.1080/14736489.2024.1234567
46. Payá Santos, C. A; Rodríguez González, V; Domínguez Pineda N. Z; Diz Casal, J; Fernández Rodríguez, J. C. & Delgado Morán, J. J. (2025). Role of the Human Factor in the Cybersecurity Ecosystem. *Journal of Information Systems Engineering and Management*,10(4). https://doi.org/10.52783/jisem.v10i4.8983
47. Payá Santos, C. A., Delgado Morán, J. J., Martino, L., García Segura, L, A., Diz Casal, J, & Fernández Rodríguez, J. C. (2023). Fuzzy Logic analysis for managing Uncertain Situations. *Review of Contemporary Philosophy* Vol 22 (1), pp. 6780 -6797. https://doi.org/10.52783/rcp.1132
48. Paya Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova,* 19(36), 1121–1136. https://doi.org/10.21830/19006586.855

49. Payá-Santos C., Delgado Morán J. J, & Mazurier P. A. (2018). Individual terrorism as a response to the distorted phenomenon of cultural identity. En J. Ramírez & G. Abad-Quintanal (Eds.), Cross-cultural dialogue as a conflict management strategy. *Advanced sciences and technologies for security applications*. Springer. https://doi.org/10.1007/978-3-319-77231-8_4
50. Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4), 1–20. https://doi.org/10.14763/2020.4.1532
51. Rajmohan, A., Singh, A., & Choudhury, T. (2025). India's digital public infrastructure and strategic autonomy. *Observer Research Foundation*.
52. Rodríguez González, V., Payá, Santos., C, A., & Peña Herrera. B. (2023). Estudio criminológico del ciberdelincuente y sus víctimas. *Cuadernos de RES PUBLICA en Derecho y criminología,* (1) 95-107. https://doi.org/10.46661/respublica.8072.
53. Sanz González, R, Luque Juárez, J. Mª., Martino, L., Liz Rivas, L., Delgado Morán, J. J., & Payá Santos, C. A. (2024) Artificial Intelligence Applications for Criminology and Police Sciences. *International Journal of Humanities and Social Science.* Vol. 14, No. 2, pp. 139-148. https://doi.org/10.15640/jehd.v14n2a14
54. Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. W. W. Norton & Company.
55. Segal, A. (2020). *China, cyberspace, and the struggle for global internet governance*. Council on Foreign Relations Press.
56. Shen, H. (2023). China's digital Silk Road and the politics of standards. *Telecommunications Policy, 47*(5), 102–135. https://doi.org/10.1016/j.telpol.2023.102718
57. Shiozawa, A. (2022). Japan's economic security strategy: Trusted connectivity and digital sovereignty. *Asia-Pacific Review, 29*(2), 67–85. https://doi.org/10.1080/13439006.2022.2109734
58. Simón, L. (2024). Europe's defense sovereignty in the shadow of war. *Survival, 66*(1), 23–46. https://doi.org/10.1080/00396338.2024.2287654
59. Standing Committee of the National People's Congress. (2021). *Data Security Law of the People's Republic of China*. Beijing.
60. State Council of China. (2021). *Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China*. Beijing.
61. State Council of China. (2023). *China Standards 2035: Strategic planning for global leadership in technology*. Beijing.
62. U.S. Congress. (2018). *National Quantum Initiative Act*. Public Law No. 115-368. https://www.congress.gov/115/plaws/publ368/PLAW-115publ368.pdf
63. U.S. Congress. (2022). *CHIPS and Science Act of 2022*. Public Law No. 117-167. https://www.congress.gov/bill/117th-congress/house-bill/4346
64. U.S. Department of State. (2024). *U.S. International Cyberspace & Digital Policy Strategy*. https://www.state.gov
65. White House. (2021). *National security strategy of the United States*. Washington, DC: The White House.
66. Zuboff, S. (2023). *The digital future: Surveillance capitalism and algorithmic power*. Harvard University Press