International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Analysis of Geopolitics of Digital Protectionism With Reference to Technological Sovereignty in India, the United States, and China

Ms. Priyanka Sinha

Research Scholar, Chanakya National Law University

Abstract:
In the digital economy, data serves as a novel factor and a principal catalyst for production and distribution processes, while digital platforms represent a new organizational structure that links many users through network effects, fostering innovation and change in established sectors. Data and digital platforms are fundamental components of digital commerce and are thus critical factors in the development of trade policy. One of the most distinguishing characteristics of the global environment in the 21st century is the geopolitics of digital protectionism, which is connected with the drive to achieve technical sovereignty. As significant digital powers, India, the United States of America, and China each approach this nexus with their own unique tactics, which are motivated by the economic, security, and political imperatives related to their own countries. The worldwide internet ecosystem is also experiencing a significant digital revolution, characterized by a rapid transition towards digital protectionism and the desire for technology sovereignty. The increasing protectionism in trade, the fragmentation of trade blocs, and geopolitical tensions are inducing disruptions and uncertainty in global supply chains. In the meantime, these transformations generate profitable opportunities for some trades and enterprises to enhance the supply chains, explore new markets, and embrace data localization. The traditional economic models are inadequately considering the impacts of abrupt policy alterations, significantly with the tariffs and capital movements. As the global economic landscape grows increasingly unstable, it is essential to understand cross-border economic dynamics in the digital era within such critical geopolitical situation. This research paper sets the objective to examine the intricate geopolitical issue, emphasizing the unique yet interrelated strategies of India, the United States, and China. Inspired by national security, economic competitiveness, and ideological dominance, these nations are progressively enacting laws that emphasize domestic digital priorities. Digital protectionism, characterized by data localization, export limits, and limitations on foreign digital services which operates not just only as a trade barrier but also as a strategic instrument for attaining greater technical free will.

Keywords: digital geopolitics, digital protectionism, data sovereignty, trade, data

The global economy is transforming as digitalization significantly expands across major technological industries, encompassing both Big Tech corporations and breakthroughs in agriculture. Nevertheless, this has also become a focal point of geopolitical conflicts, prompting the implementation of specific digital

protection measures that can serve both as a shield and a weapon against the digital economies of other nations. The geopolitical dynamics between the United States and China become the focal point for study and research about data protectionism and technical sovereignty. This research paper aims to examine the geopolitical tensions stemming from technological sovereignty and the extent to which it has been implemented by major economic nations, with particular reference to the current Indian context regarding the digital economy and digital protection.

In the 21st-century global context, the geopolitics of digital protectionism has merged with the notion of technological sovereignty.[1] As major digital powers, countries like the US and China each have an axis with aspects drawn from economic security and political imperatives. As India has also emerged as a digital power and a major digital consumer, it has also developed certain strategies driven by economic, political, and security purposes. However, the key terminologies, such as digital protectionism and technological sovereignty, have different distinct meanings.[2]

The terms may appear to define the same concept at first glance; however, on a global scale, they embody distinct characteristics. Technological sovereignty pertains to a nation that seeks to safeguard its technological innovations within its borders or limit the influx of technological advancements from other nations to local confines. Digital protection encompasses the actions a government can implement to safeguard its domestic sectors and data transfers. Whereas digital protection is done through the measures that can be taken by a nation to protect the domestic industries and data flows. Foreign technological companies' influence is restricted within their borders.

Digital protectionism also resembles the concept of data localization requirements as well as the control of cross-border data flows, discriminatory taxation, barriers to market access for foreign tech firms, and local content mandates. Technological sovereignty refers to a nation's capacity to autonomously control and deploy vital technologies or to access them without reliance on unilateral agreements. It guarantees a nation's ability to shape its own digital destiny and enact legislation for protection. It protects the nation's economic, social, and national security interests moving forward. It limits foreign entities' control and prevents excessive influence on critical technological infrastructure and capacities. Digital protectionism and digital sovereignty are becoming increasingly significant components of trade policy, especially for countries such as India that seek to reconcile economic progress with national interests in the digital domain. Digital protectionism denotes governmental actions aimed at safeguarding domestic digital sectors from international competition, whereas digital sovereignty pertains to a nation's authority over its digital infrastructure, data, and online operations. Protectionism in the digital economy is characterized by actions and policies taken by the government that give priority to the preservation of national interests within the digital economy. In order to restrict or control the flow of digital goods, services, data, and information across international borders, several measures have been implemented.[3] From a conceptual standpoint, it is possible to understand it as an extension of classical protectionism, which is characterized by the use of taxes and quotas on tangible commodities, into the realm of digital technology. For instance,

[1] The Geopolitics of Trade: Diverging Digital Governance Threatens Data Flows - Stratfor, accessed July 5, 2025, https://worldview.stratfor.com/article/geopolitics-trade-diverging-digital-governance-threatens-data-flows

[2] The geopolitics of technology: How the EU can become a global player | ECFR, accessed July 5, 2025, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/

[3] Law.stanford.edu, accessed July 5, 2025, https://law.stanford.edu/transatlantic-technology-law-forum/projects/the-rise-of-digital-protectionism-eu-us-comparative-perspectives/#:~:text=Digital%20protectionism%2C%20characterized%20by%20the,%2C%20economic%2C%20and%20technological%20shifts.

rather than levying taxes on steel that is imported, a nation can set restrictions that require data that is generated within its boundaries to be stored within the territories of the nation.. Digital protectionism involves not just explicit policy instruments but also the subtle effects of regulatory frameworks, technology standards, and even cybersecurity protocols when these are purposefully deployed to further nationalistic goals.[4]

Sovereignty over technology means a nation or group of nations can choose, create, acquire, use, improve, and profit from the technologies that are crucial to new manufacturing processes.[5] The ability of a nation to achieve its political and social agendas without being hampered by inadequate or insufficient control over essential technology is what it means to have this capability. Since total autonomy is impractical in the modern, globally interdependent technology environment, especially in the field of information and communication technology (ICT), this idea stands apart from technological autarchy and self-sufficiency.[6] Instead, technical sovereignty places an emphasis on the requirement that a nation, or a federation of nations, such as the European Union[7], must either create or retain a high degree of autonomy or the lowest feasible level of dependence for fundamental technologies.[8] Data sovereignty, cyber sovereignty, and digital sovereignty are all meaning the same thing: the ability of a nation to decide what happens to its data, hardware, and software in the digital realm.[9] An effective reason for digital protectionism that is being claimed more and more frequently is the protection of national security.[10] Protecting vital digital infrastructure, reducing the dangers of foreign monitoring, and preventing illegal access to sensitive information are all reasons why governments are trying to increase their control over data. National security is of the utmost importance in the modern power struggle because of the weaponization, mastery, and control of digital technology. However, when it comes to digital protectionism, the wider interpretation of "national security" as a reason has become an influential narrative. This interpretation empowers governments to justify policies that might otherwise be regarded as being solely protectionist.[11]

In pursuit of digital protectionism and technical sovereignty goals, nations utilize a wide range of policy tools:

- **Data Localization:** The standards that ensure that data gathered inside a nation's boundaries must be retained and handled domestically. These constraints establish barriers in the digital realm, oftentimes empowering domestic sectors or meet certain national goals.

[4] Digital Protectionism → Term - Climate → Sustainability Directory, accessed July 9, 2025, https://climate.sustainability-directory.com/term/digital-protectionism/

[5] TECHNOLOGICAL SOVEREIGNTY: FORGOTTEN FACTOR IN THE 'HI-TECH' RAZZAMATAZZ - ScienceOpen, accessed July 9, 2025, https://www.scienceopen.com/hosted-document?doi=10.1080/08109028308628930

[6] Ibid

[7] Coopetitive Technological Sovereignty: A Strategy to Reconcile International Collaboration with Knowledge and Economic Security - Intereconomics, accessed July 10, 2025, https://www.intereconomics.eu/contents/year/2025/number/2/article/coopetitive-technological-sovereignty-a-strategy-to-reconcile-international-collaboration-with-knowledge-and-economic-security.html

[8] Technological Sovereignty: - VDE, accessed July 10, 2025, https://www.vde.com/resource/blob/2013656/66f71138ba34b7b3ad0e2aa248b71abd/vde-position-paper technological-sovereignty-data.pdf

[9] What is digital sovereignty and how are countries approaching it? | World Economic Forum, accessed July 11, 2025, https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[10] The Geopolitics of Trade: Diverging Digital Governance Threatens Data Flows - Stratfor, accessed August 5, 2025, https://worldview.stratfor.com/article/geopolitics-trade-diverging-digital-governance-threatens-data-flows

[11] The geopolitics of technology: How the EU can become a global player | ECFR, accessed August 5, 2025, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/

- **Content Regulation and Censorship:** In order to restrict or filter access to foreign websites, apps, or content that is available on the web, governments can decide to enact guidelines. Beyond monetary concerns, this serves to regulate the flow of information and protect national principles.
- **Controls on exports:** These policies necessitate preventing other countries from gaining access to essential technological advances. They are utilized in a strategic manner specifically for the purpose of advancing protectionist agendas and maintaining technical advantages, particularly in sensitive industries.
- **Investment Screening:** This involves maintaining significant investments in the technology sector for the purpose to minimize the likelihood of possible breaches of security. The Committee on Foreign Investment in the United States (CFIUS), which examines foreign acquisitions with the purpose of determining whether or not they have consequences for national security, is a striking example.[12]
- **Procurement process:** Domestic digital enterprises are given preferential consideration in government procurement processes under these regulations. These kinds of policies are a weapon that may be used to encourage innovation within the country and to protect vital supply networks.[13]
- **Digital Services Taxes:** The taxes are levied on the revenues that digital services produce from consumers inside the jurisdiction where they operate, regardless of the company's worldwide headquarters. These taxes take effect on the revenues generated by digital services. Individuals frequently consider them to be a reaction to what they believe to be unfair competition and tax evasion on the part of global digital firms.

In the context of the rising geopolitical struggle over technology and data, these three countries represent a variety of approaches to digital governance and are at the centre of the competition. The various techniques, objectives, and policy instruments that each of them employs provide a fascinating comparative lens through which to examine the intricate relationship between technological sovereignty and digital protectionism.[14] Protectionism has a long and storied history in India, with import limits being initially established during World War II and then subsequently tightened by communist administrations after the country's independence in order to safeguard native businesses. As a result of this historical approach, the nation frequently became uncompetitive and experienced recurrent problems in its balance of payments, which ultimately resulted in the need for economic liberalization in the year 1991.[15] In spite of these transformations, the "Make in India" program that is currently being implemented by the present administration continues to place an emphasis on bolstering domestic production and consumption. Increasing the proportion of the gross domestic product that is contributed by manufacturing is the stated objective of this program, which intends to create a climate that is favourable to investments, construct modern infrastructure, and open up new industries to foreign capital.[16] The remarkable amount of progress has been achieved by the "Make in India" initiative to develop the electronic systems industry, most notably in the manufacturing of smartphones, despite the fact that it has encountered difficulties in meeting

[12] Committee on Foreign Investment in the United States (CFIUS ..., accessed July 18, 2025, https://www.congress.gov/crs-product/IF10177
[13] UK-India CETA Chapter 15: Government Procurement - GOV.UK, accessed July 16, 2025, https://www.gov.uk/government/publications/uk-india-ceta-chapter-15-government-procurement
[14] Ibid
[15] India vs Trump: Three choices and a teachable moment, accessed July 15, 2025, https://economictimes.indiatimes.com/opinion/et-commentary/while-india-is-a-friend-grump-gives-us-his-stare/articleshow/123003845.cms
[16] Make in India - Wikipedia, accessed July 15, 2025, https://en.wikipedia.org/wiki/Make_in_India

its total manufacturing GDP targets. As of 2019, 95% of cell phones sold in India were manufactured domestically, which is a considerable rise over the 19.9% that was produced domestically in 2015. Several big worldwide corporations, including Foxconn, Pegatron, and Samsung, have made significant investments as an outcome of this performance of this initiative.[17]

In addition to the 'Make in India' mission, the National Telecom Policy 2025 (from this point forward-NTP-25) establishes an ambitious vision for India's digital future, with the goal to promote the country not just as a top consumer, but also as a reputable worldwide provider of telecom goods and services. With the help of the NTP-25, India aims to double the share of its telecom sector to the country's GDP by 2030 and to invest heavily in the telecom industry every year by increase the number of telecom startups and exports by the same amount, and boost research and development spending on emerging technologies like 5G/6G, AI, the Internet of Things, and quantum communications by a large margin.[18] The India Semiconductor Mission, which was established in 2021, would further strengthen this push for technological independence. This mission offers significant financial aid, providing up to 50% funding for the creation of semiconductor manufacturing display panel manufacturing process, and chip design facilities.[19] The aim is to enhance India's incorporation into global electronics value chains and diminish its reliance on imports for essential components. The objective prioritizes talent development, aiming to train 85,000 engineers in advanced semiconductor and electronics production.[20] These industrial restrictions, especially in the telecommunications and semiconductor industries, signify a strategic shift for India from general protectionism to focused techno-nationalism. India seeks to establish fundamental competencies necessary for attaining true technology sovereignty by focusing on vital digital infrastructure and components. This strategy aims to mitigate susceptibility to global supply chain interruptions and geopolitical tensions, regardless of the complete achievement of the overarching "Make in India" manufacturing objectives. The focus on indigenous development in these strategic domains indicates a nuanced comprehension of technology as a crucial foundation of national strength and strategic independence.

A case study on the prohibition of Chinese applications and its geopolitical ramifications. In June 2020, subsequent to military confrontations along the India-China border, the Indian government prohibited 59 Chinese applications, including widely used platforms such as TikTok and WeChat. The formal rationale for this measure was that these applications were "detrimental to the sovereignty and integrity of India, the defense of India, state security, and public order."[21] This prohibition has considerable geopolitical ramifications. It conveyed a definitive message of defiance against perceived Chinese hegemony in the area, uniting India with other democracies, including the United States and Japan, to establish a

[17] Ibid.

[18] It is requested to provide the comments/suggestions/feedback, if ..., accessed July 25, 2025, https://avantiscdnprodstorage.blob.core.windows.net/legalupdatedocs/44839/DoT-issued-the-Draft-National-Telecom-Policy-NTP-2025-for-Public-Consultation-July232025.pdf

[19] Semiconductor mission pushes India from being aspirant to ..., accessed July 25, 2025, https://m.economictimes.com/industry/cons-products/electronics/semiconductor-mission-pushes-india-from-being-aspirant-to-becoming-global-powerhouse/articleshow/123084531.cms

[20] Press Note Details: Press Information Bureau - PIB, accessed July 25, 2025, https://www.pib.gov.in/PressNoteDetails.aspx?id=154968&NoteId=154968&ModuleId=3

[21] (PDF) Media, digital sovereignty and geopolitics: the case of the ..., accessed July 14, 2025, https://www.researchgate.net/publication/370939029_Media_digital_sovereignty_and_geopolitics_the_case_of_the_TikTok_ban_in_India

counterbalance to China's regional aspirations.[22] It was also a symbolic step towards lessening India's economic dependency on China's manufacturing and trading capabilities. The decision was made with the intention of fostering a digital ecosystem that is more self-sufficient and diversifying trade partnerships. The restriction specifically targeted apprehensions about Chinese technology firms possibly gathering sensitive information on Indian customers and transmitting it to the Chinese government, so aiming to safeguard national security and uphold data privacy for people.[23]
The prohibition of the Chinese app serves as a compelling example of digital protectionism, influenced by intricate factors such as national security concerns, economic nationalism, and direct geopolitical tensions.
It clearly illustrates that digital platforms, despite their fundamentally global character, are significantly influenced by international relations and may be utilized as instruments of statecraft. The prohibition also stimulated the development and expansion of indigenous digital alternatives, like Josh, MX TakaTak, and Koo, so bolstering the "Atma-Nirbhar Bharat" (self-reliant India) and "Digital India" initiatives. This result highlights how protectionist policies may foster national technical sovereignty, albeit it may compromise market openness and contribute to digital fragmentation. The gathering also underscored an increasing "techno-nationalist" zeal in India. [24] India's strategy for digital sovereignty is a multifaceted and dynamic amalgamation of economic nationalism and national security considerations. It signifies a shift from a historical tradition of extensive protectionism to a more focused and sophisticated approach.[25]
The digital protectionism of digital sovereignty of US have a different approach, historically, the United States has fervently supported the unrestricted movement of data across international boundaries, promoting an open, interoperable, dependable, and secure internet.[26] The U.S. Trade Representative's office has been diligently cataloguing digital trade barriers, such as data localization requirements, burdensome technology standards, demands for source code disclosure, and restrictions on internet services, in an effort to identify and reduce these obstacles for American companies worldwide.[27]
However, a notable shift in US strategy has been increasingly apparent. The United States is currently advancing its data controls and other limitations, specifically aimed at select "countries of concern," principally under the framework of national security. The evolution of this strategy is propelled by escalating geopolitical competition, particularly with China, resulting in the acknowledgment that even staunch advocates of digital openness would prioritize national security and technical supremacy in the presence of strategic adversaries. The United States aims to mitigate the influence of China and Russia while maintaining its technical pre-eminences in critical domains, including military artificial intelligence.

[22] The Ban on Chinese Apps: A Chasm in the Indo-Chinese ..., accessed July 15, 2025, https://pallavisareen.com/the-ban-on-chinese-apps-a-chasm-in-the-indo-chinese-relationship/
[23] Ibid
[24] (PDF) Media, digital sovereignty and geopolitics: the case of the ..., accessed July 14, 2025, https://www.researchgate.net/publication/370939029_Media_digital_sovereignty_and_geopolitics_the_case_of_the_TikTok_ban_in_India
[25] India's Digital Sovereignty - NEXT IAS, accessed July 21, 2025, https://www.nextias.com/ca/editorial-analysis/02-08-2025/india-digital-sovereignty
[26] NATIONAL CYBER STRATEGY - Trump White House Archives, accessed July 23, 2025, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[27] Key Barriers to Digital Trade - USTR, accessed July 22, 2025, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade

This strategic rivalry, defined as a new era in the National Cyber Strategy, requires policy actions that might impose penalties on malicious cyber actors.[28]

Tackling China's access to and development of sophisticated computer and semiconductor manufacturing products, the United States imposed extensive new export restrictions on October 7, 2022.[29] Concerns over China's military use of sophisticated semiconductors, the need to dominate in AI, and the need to limit human capital flow to China's semiconductor sector drive these constraints.[30] The prohibitions apply to a variety of semiconductors and related equipment, including logic chips (16nm/14nm or lower), DRAM memory chips (18nm half-pitch or fewer), NAND flash memory chips (128 layers or more), and assistance given by US citizens to production facilities in the PRC.[31] U.S. export restrictions are an example of aggressive digital protectionism since they use vital technology supply chains as a weapon to slow down a competitor's innovation. China is now only a negligible manufacturer of sophisticated AI chips, according to early research, because these regulations have drastically reduced the country's chipmaking capacity. Chinese labs have still been able to make highly competitive AI models, though it may be harder to use them on a large scale because of the controls.[32] US corporations like Synopsys and Cadence must stop operations in China or get sales permits.[33] This strategy encourages global technology decoupling, requiring states to build parallel, possibly less efficient supply chains and fragmenting the global digital economy. The US is directly involved in geoeconomics, where economic interdependencies are leveraged to safeguard geopolitical goals, by restricting access to vital technology and embargoing sensitive technologies.[34] This strategic action protects the US market and aggressively constrains a competitor's technical environment, causing worldwide ripple effects and a split global tech order. The CHIPS Act[35] is a significant piece of legislation in the United States, which allocates funds to semiconductor manufacturing and also boosts research and workforce development, which focuses on domestic supplies. The purpose of this act is to rejuvenate the US semiconductor industry and reduce dependence on foreign supply chains, thereby enhancing national security against Chinese technological advancements. The subsidizing of domestic production and putting conditions on other foreign countries has resulted in the active remodelling of global supply chains and the technology and the minimizing of the reliance on foreign technology. All the steps that have been taken by the US government are to boost the domestic industries and disturb the field and to ensure national security in certain critical technological sectors. These steps not only show the national security in technological advancements but also the restricted openness of the US's global tech ecosystem.

[28] NATIONAL CYBER STRATEGY - Trump White House Archives, accessed July 25, 2025, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[29] United States New Export Controls on Advanced Computing and ..., accessed July 25, 2025, https://en.wikipedia.org/wiki/United_States_New_Export_Controls_on_Advanced_Computing_and_Semiconductors_to_China
[30] ibid
[31] ibid
[32] How US Export Controls Have (and Haven't) Curbed Chinese AI | AI ..., accessed July 25, 2025, https://ai-frontiers.org/articles/us-chip-export-controls-china-ai
[33] Technology Transfers in response to US Export Controls | Article ..., accessed July 25, 2025, https://chambers.com/articles/technology-transfers-in-response-to-us-export-controls
[34] The geopolitics of technology: How the EU can become a global player | ECFR, accessed July 25, 2025, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/
[35] The Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022.

Similarly, The CLOUD Act, 2018[36] empowers the US government to observe US-based technology businesses' electronic data headquartered on foreign servers.[37] The Act has wide impact beyond promoting access to digital evidence for grave crimes being investigated by global partners under some bilateral arrangements which provides in the process they must respect privacy and civil rights provisions.[38] The CLOUD Act gives the US worldwide data jurisdiction. A possible conflict arises as a result of this with the data sovereignty claims of other governments, who are progressively mandating the localization of data.[39]

Another America's policy for procurement which prefer domestic technology is The Buy American Act and Information Technology Act (SHARE IT Act)[40], enacted in 2024. In order to encourage federal agencies in the United States to acquire items that are in accordance with domestic preference standards, the Buy American Act imposes a price penalty on products that are imported from other countries. In the case of manufactured goods, the BAA stipulates that the item must be produced in the United States, and the cost of its components originating from the United States must be greater than 55% (a level that is scheduled to climb to 75% by the year 2029).[41] The SHARE IT Act, passed into law in 2024, mandates that federal agencies must store and share source code that was developed specifically for them. The source code must be stored in either public or private repositories that are accessible throughout the government.[42] The United States is aggressively cultivating its own technology base through the implementation of these procurement rules, which include the creation of a preferred market for domestic digital goods and services, as well as the promotion of the internal development and reuse of software. The purpose of this strategy is to lessen the state's reliance on commercially available solutions from other countries and to construct a digital infrastructure that is independent of the state. This will contribute to the state's technological sovereignty by ensuring that it maintains control over the digital tools and systems that are essential to the functioning of the government and to the protection of the nation.

The implications on US AI prioritizing domestic leadership performs as an extensive policy framework aimed at eliminating regulatory obstacles, substantially enhancing US investment in AI infrastructure and expertise, and establishing US dominance in international AI markets.[43] The plan expressly intends to increase AI exports to alliance nations while restricting AI technology and components for the rivals countries.[44]This AI Action Plan is comprehensive and optimistic, linking AI leadership to national competitiveness and security. This demonstrates a complex strategy to technical sovereignty that is both

[36] The Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.
[37] US Cloud Act - Palo Alto Networks, accessed August 1, 2025, https://www.paloaltonetworks.com/legal-notices/trust-center/us-cloud-act
[38] Criminal Division | CLOUD Act Resources - Department of Justice, accessed August 1, 2025, https://www.justice.gov/criminal/cloud-act-resources
[39] Data localization - Wikipedia, accessed August 1, 2025, https://en.wikipedia.org/wiki/Data_localization
[40] Source Code Harmonization and Reuse in Information Technology Act, 2024.
[41] An overview of Federal Laws relating to Domestic Content ..., accessed August 1, 2025, https://www.trade.gov/sites/default/files/2022-07/FederalProcurement1.pdf
[42] SHARE IT Act Requires Agencies to Share Custom-Developed Source Code Throughout the Government, accessed August 1, 2025, https://govcon.mofo.com/topics/share-it-act-requires-agencies-to-share-custom-developed-source-code-throughout-the-government
[43] A New Era for U.S. AI Policy: How America's AI Action Plan Will ..., accessed August 1, 2025, https://www.consumerfinancemonitor.com/2025/07/28/a-new-era-for-u-s-ai-policy-how-americas-ai-action-plan-will-shape-industry-and-government/
[44] A New Era for U.S. AI Policy: How America's AI Action Plan Will ..., accessed August 2, 2025, https://www.consumerfinancemonitor.com/2025/07/28/a-new-era-for-u-s-ai-policy-how-americas-ai-action-plan-will-shape-industry-and-government/

offensive (boosting AI exports) and defensive (restricting rivals) in nature. This twin strategy reinforces AI as a geopolitical battlefield. This approach highlights AI's dual-use nature and its substantial consequences for national power, making AI governance a critical geopolitical issue and a major driver of digital protectionism.

The "Great Firewall" (GFW) of China is an intricate structure that brings together legal regulations and technical advancements with modern technology adopted by the People's Republic of China to control its domestic cyberspace.[45] This broad framework deliberately restricts access to many foreign digital services, including prominent ones like as Google and Facebook.[46] It utilizes extensive content-filtering tools, including IP blocking, packet filtering for sensitive keywords, and sophisticated technologies such as voice and face recognition.[47] Baidu, China's dominant internet search engine, incorporates extensive restrictions in its search algorithms.[48] The GFW's principal aims are to protect Chinese citizens from external influence and to rigorously regulate the dissemination of information domestically.[49] The Great Firewall exemplifies China's state-centric digital protectionism, demonstrating that information control and restriction are fundamental to its philosophy of "digital sovereignty." This framework safeguards local technology firms from international competition while simultaneously functioning as an essential mechanism for preserving societal unity and political stability, illustrating a clear correlation between digital policy and authoritarian rule. The pervasive governmental control and systematic filtering characteristic of this approach, as evidenced by successful local alternatives such as VKontakte and TikTok under authoritarian regimes, result in considerable limitations on individual liberties.[50] China's Digital Silk Road (DSR) advances the global expansion of the "state-centric internet governance model" by selling surveillance technologies reminiscent of the "Great Firewall".[51] This illustrates that for China, digital protectionism is tightly linked to national security.

China's Cybersecurity Law (CSL), passed in 2017, aims to improve privacy of data and localization, and cyber security measures for national security.[52] The CSL requires "network operators" such as social media platforms, app developers, and other technological companies which retain the personal information obtained by Chinese servers.[53] Cross-border transfers of information required the government consent and other procedural requirements along with User identification information which are also required for network access, domain name registration, and other services by law.[54]

Additionally, the CSL mandates that any acquisitions of foreign software or hardware made by government agencies or "critical information infrastructure operators" must be subjected to a national

[45] Great Firewall - Wikipedia, accessed August 2, 2025, https://en.wikipedia.org/wiki/Great_Firewall

[46] China and the United States: Digital Protectionism vs. Digital Free Trade | ITIF, accessed August 2, 2025, https://itif.org/publications/2019/10/18/china-and-united-states-digital-protectionism-vs-digital-free-trade/

[47] China's Great Firewall - CS Stanford, accessed August 2, 2025, https://cs.stanford.edu/people/eroberts/cs181/projects/201011/FreeExpressionVsSocialCohesion/china_policy.html

[48] Ibid.

[49] The geopolitics of technology: How the EU can become a global player | ECFR, accessed August 3, 2025, https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player/

[50] How US Export Controls Have (and Haven't) Curbed Chinese AI | AI ..., accessed August 3, 2025, https://ai-frontiers.org/articles/us-chip-export-controls-china-ai.

[51] The Digital Silk Road: Implication Of China's Techno-Political ..., accessed August 3, 2025, https://www.lifeofsoldiers.com/2025/02/20/the-digital-silk-road-implication-of-chinas-techno-political-strategy/

[52] What are China's Data Localization Rules? Requirements for ..., accessed August 5, 2025, https://www.ud.hk/insight/article/What-are-the-Data-Localization-Rules-in-China

[53] Ibid.

[54] Cybersecurity Law of the People's Republic of China - Wikipedia, accessed August 5, 2025, https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China

security evaluation. This examination may require the surrender of source code as well as other sensitive proprietary information.[55] Chinese officials can also spot-check enterprise network operations. The CSL, DSL,[56] and PIPL[57] comprise a state-centric data governance system that prioritizes national security and data flow management.[58] Despite its strict data protection claims, this method was widely criticized for damaging international firms and allowing government spying. Apple and Microsoft have invested in local data canters to comply, but Skype and WhatsApp have been restricted. A sophisticated type of digital protectionism, the CSL uses national security and data protection narratives to limit digital activity within its boundaries. The result is a fragmented digital environment where China's domestic data is segregated and regulated, solidifying its technical sovereignty and allowing it to externalize its digital governance model to other countries.[59]

Several policies and laws enacted in China for Indigenous Innovation, one of them is "Made in China 2025" (MIC 2025) which was launched in 2015 aims to modernize its industrial capabilities and make it an internationally recognized leader in high-tech sectors. This effort aims at minimizing China's being reliant on foreign technology by aggressively encouraging local inventions and growing global-competitive Chinese firms. Technology-related businesses including AI, 5G, aerospace, semiconductors, electric cars, and robots are among the ten targeted industries. The main Focus is on reaching 70% Chinese-domestic core materials by 2025.64 The concept is supported by hundreds of billions of dollars in funding from the government from loans with low interest rates, tax cuts, and other subsidies.[60] MIC 2025 is more than just a defensive protectionist policy; it's a grand plan to achieve complete technical sovereignty and world domination. China wants to dominate the value chain from Development and research to manufacture by investing in as well as indigenizing essential technology. This state-driven strategy intensifies global tech competitiveness and accelerates the creation of technology swirls to influence technological sovereignty with tireless commitment by China. The fierce technical battle for industrial domination, especially between China and the US, drives these kinds of methods.[61]

In order to regulate the export and import of technological goods, China has two main mechanisms. First, the Export Control Law, which was passed in December 2020, is mainly responsible for regulating the export of dual-use technology and military technology exported from the country. The law consolidates regulations governing dual-use, military, and the nuclear technology, while also establishing extraterritorial jurisdiction and reciprocal measures that reflect US-style limitations. The second system is involved with the Foreign Trade Law and its related Rules and Regulations, which outline the import and export of civilian technology. Within the civilian technology framework, imported and exported technologies are classified as "free," "restricted," or "prohibited." Technologies which are classified as

[55] Ibid.
[56] Data Security Law.
[57] Personal Information Protection Law.
[58] China Privacy & Data Protection - Cyber Security Law; Data Security Law; Personal Information Protection Law - Bird & Bird, accessed August 5, 2025, https://www.twobirds.com/en/trending-topics/china-privacy-and-data-protection
[59] Cybersecurity Law of the People's Republic of China - Wikipedia, accessed August 5, 2025, https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
[60] Made in China 2025 - Wikipedia, accessed August 5, 2025, https://en.wikipedia.org/wiki/Made_in_China_2025
[61] Coopetitive Technological Sovereignty: A Strategy to Reconcile International Collaboration with Knowledge and Economic Security - Intereconomics, accessed August 5, 2025, https://www.intereconomics.eu/contents/year/2025/number/2/article/coopetitive-technological-sovereignty-a-strategy-to-reconcile-international-collaboration-with-knowledge-and-economic-security.html

"restricted" may only be traded with a license granted by the appropriate foreign trade authority.[62] China's enactment of its own export curbs, especially those paralleling US measures, signifies a fortification of its techno-nationalist position and an inclination to participate in a reciprocal "tech war." This action pertains not only to safeguarding national security but also to establishing leverage and showcasing the ability to retaliate in the current geopolitical rivalry. The Export Control Law's incorporation of "reciprocal measures mirroring U.S.-style restrictions" obviously signifies a deliberate reaction to U.S. export controls.[63] This reinforces the trend toward a divided global technological ecosystem, where strategic rivalry increasingly supersedes economic efficiency and international collaboration.

Conclusion

The primary objective is to guarantee that India's digital future is determined by its own national interests, rather than being influenced by global technology corporations or foreign governments. The journey has obstacles, such as the necessity to create effective indigenous alternatives for specific digital services, manage legislative ambiguities, and maintain a careful equilibrium between global digital integration and the quest for self-sufficiency. This fundamental transformation, aimed at safeguarding US interests, exacerbates the global fragmentation of the internet and undermines the international rules formerly advocated by the US, resulting in a more unpredictable global digital environment. In the digital sphere, US policy is shifting from a free-market worldview to one that is more strategic and security-driven. Whereas the combination of proactive digital protectionist policies like export limits and AI export promotion and reactive policies like strong investment screening through CFIUS, the CHIPS Act, and government procurement preferences characterize this trend. The major goal is to safeguard vital supply chains while continuing to be technologically leading, especially with China's rivalry heating up. The digital sovereignty model of China is distinctly state-centric, emphasizing national control and technology self-sufficiency via comprehensive regulatory frameworks, assertive industrial strategies, and broad global efforts. This holistic strategy seeks technical supremacy, frequently resulting in considerable market distortions and eliciting apprehensions over digital dictatorship. India, the United States, and China possess intrinsic motives for their endeavours in digital protectionism and technical sovereignty. The primary factors are national security, economic competitiveness, and the quest for technical supremacy. Each utilizes a combination of policy instruments, including data localization, content regulation, investment scrutiny, and incentives for domestic production. The joint endeavour of these major countries towards digital protectionism, intended to safeguard perceived national interests and technical autonomy, is resulting in a less efficient, more politicized, and increasingly fragmented global digital economy. This fragmentation appears as a "splinternet" or "digital balkanization," where differing national digital governance frameworks and escalating barriers to digital trade generate a more intricate regulatory landscape for digital commerce and cross-border data transfers. This fragmentation incurs substantial compliance expenses and operational difficulties for global corporations striving to function across many countries. It also jeopardizes overall economic progress and obstructs global innovation, disproportionately disadvantaging smaller enterprises. it has been contended that digital protectionism,

[62] FAQs regarding China Technology Import and Export Control - KWM, accessed August 5, 2025, https://www.kwm.com/cn/en/insights/latest-thinking/faqs-regarding-china-technology-import-and-export-control.html
[63] United States New Export Controls on Advanced Computing and ..., accessed August 5, 2025, https://en.wikipedia.org/wiki/United_States_New_Export_Controls_on_Advanced_Computing_and_Semiconductors_to_China

despite assertions of promoting home innovation, ultimately obstructs global commerce, limits consumer options, and undermines economic efficiency. Geopolitical tensions and trade conflicts intensify this fragmentation, prompting nations to exert further control over supply chains, especially in essential technology such as semiconductors. This concept promotes the onshoring or "friendshoring" of production, emphasizing security and strategic benefit rather than mere market efficiency. The cumulative impact signifies a structural transition from a globally linked, open internet to a fragmented digital environment. This jeopardizes the fundamental foundations of the cyberspace as a transcendent platform for trade and knowledge. It is possible to draw the conclusion that, although every nation may notice a surge in the sense of security or the development of local digital sectors, the collective result may constitute a global digital economy that can be less innovative, less efficient, and more politically sensitive. This can happen as the strategic decoupling may become an established trend, which can force businesses to negotiate with systems of regulation that can be highly incompatible with one another, which may ultimately result in elevated expenses and a weakened global reach.