CASS

CENTRE for AEROSPACE & SECURITY STUDIES

Tech Globalism and Tech Realism: Navigating the Digital Divide

Syed Ahmed Ali

Research Assistant

Working Paper

President
Air Marshal Javaid Ahmed (Retd)

Edited by:
Mashal Shahid

Proofreading & Reference Standardisation
Mashal Shahid

Layout
Syed Ahmed Ali

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

+92 051 5405011
cass.thinkers@casstt.com
cass.thinkers
cassthinkers
@CassThinkers
Centre for Aerospace & Security Studies

CENTRE for AEROSPACE & SECURITY STUDIES

Tech Globalism vs. Tech Realism: Navigating the Digital Divide

Working Paper

Syed Ahmed Ali

Research Assistant

TABLE OF CONTENTS

Abstract

The research paper is an explorative study that aims to understand tech globalism and tech realism and how they relate to the modern technoscape. The study has two goals: firstly, it aims to understand the theoretical foundations of both these perspectives. Secondly, the research wants to investigate the nature of technoscape, whether it aligns more closely with tech realism or globalism. Through comparative analysis, the study found that while techno-globalism fostered cooperation through international institutions such as the ITU, TRIPS, and similar initiatives. Techno-realism, on the other hand, peddled competition as evident by practices such as tech denial, tech censorship, a separate internet connection, and exclusive access to international digital markets. Analysing the modern technoscape, the research found that while the volume of cross-data flow has increased manifold, states have also placed restrictions. This is to safeguard their national security against perceived threats and preserve digital sovereignty. Technological diffusion across borders is subject to sensitivity to state interests and security. Low-tech products usually don't face restrictions like high-tech products, which are subjected to export controls, supply chain constraints, and trade barriers. The restrictions on tech-related trade have started polarisation, where new tech ecosystems are developing. There is a great disparity in internet connectivity between the developing and developed countries, limiting equal growth opportunities. Analysing these results, the research concludes that the technoscape is oscillating between managed interdependence and tech blocs. The final result is subject to international law and cooperation

Keywords: Technoscape, Tech Realism, Tech Globalism, Digital Divide, Tech Ecosystem

Introduction

The 21st century is marked by a technological boom, where nation-states compete globally in a technological race in pursuit of resources, markets. The complexity of the technological landscape compels nation-states to balance idealistic globalism and pragmatic, conflict-driven realism. As the modern world has become increasingly interconnected through the use of digital technologies, a digital divide has emerged, restricting who can fully participate. This creates a class which is left behind and cannot fully benefit from the advantages of digital connectivity. This means that areas with less technological connectivity face disadvantages that stagnate economic growth. On the other hand, nation-states limit access to technology to ensure their political control or reduce technological vulnerabilities to rival nation-states. The debate of technological globalism and realism, in effect, reflects the complex dynamics of global politics.

Technological globalism envisions a world where technology can act as a unifying force that promotes global cooperation, economic growth, and the free flow of information. It also advocates for universal access to technology, open systems, and global technological advancements. Technological realism, on the other hand, challenges digital access, advocates cyber sovereignty, and prioritises national interests over global connectivity. Digital politics is not limited to the digital divide; it extends to control over the infrastructure, governance, and technological standards.

This research paper aims to help navigate the tension of technological globalism and realism in the complex techno-geopolitical landscape. The study will focus on the technological cooperation as well as competition that exists in the technoscape. The paper will also examine the role of international institutes in the interactions of states. For the analysis of competition, the study will focus on the technological race between Washington and Beijing as a core part of techno-realism commentary. The research will investigate this debate on the following lines: how does technological globalisation influence global cooperation, how does political realism shape techno realism, and what is the nature of the technoscape from the perspective of tech globalism and tech realism. The study contends that politics will determine whether nation-states will adopt cooperative or competitive behaviour.

Methodology

The research is an explorative study as it aims to understand the theoretical principles of tech globalism and realism.[1] The research has employed a comparative theoretical analysis method. This methodology is ideal for testing new theories that have not been

[1] Bernd Reiter, "Theory and Methodology of Exploratory Social Science Research," *International Journal of Science and Research Methodology* 5, no. 4 (2017): 129–150, https://digitalcommons.usf.edu/gia_facpub/132/?utm_source=digitalcommons.usf.edu%2Fgia_facpub%2F132&utm_medium=PDF&utm_campaign=PDFCoverPages.

studied before. The research paper will test these theories in the light of case studies, analysed from the perspective of tech realism and globalism. This will allow the researcher to explore how these theories function in the modern technoscape.[2]

Comparative studies are essential for theoretical development as they allow the research community to compare and contrast two different worldviews about the technoscape. This research, in particular, will use specific examples of the tech race between the US and China to understand tech realism. For tech globalism, the research will study how international institutions foster technological cooperation, global connectivity, and the sharing of ideas. It should be noted that the research cannot realistically provide an exhaustive list of all instances of technological cooperation and competition. The research will provide the theoretical perspective of techno realism and globalism about the nature of the modern technological landscape.[3] The case studies of technological cooperation and competition can provide useful theoretical insights. These insights can lay the theoretical foundation of tech realism and tech globalism, from which further inquiry can be conducted about more specific segments of the technological landscape.[4]

The research paper will focus on the investigation of the nature of the technoscape, not on the policies of individual states. The case studies cited in the research are examples of tech globalism and realism, not state policy. Due to limitations in word capacity, the paper will not cite all examples of tech globalism and realism. Instead, the individual case studies serve as examples of trends in the wider global technoscape.

Theoretical Framework of Tech Realism and Tech Globalism

This section of the research paper will lay down the theoretical foundations of tech globalism and realism. It will provide the framework of how each perspective views the modern technoscape.

Tech Globalism

The term 'tech globalism' refers to the idea that global interconnectivity and communication lead to greater technological advancements and diffusion. This means that when the global society exchanges ideas and techniques, it dramatically increases

[2] Mala Htun and Francesca Jensenius, "Comparative Analysis for Theory Development," in *Rethinking Comparison: Innovative Methods for Qualitative Political Inquiry* (Cambridge: Cambridge University Press, 2021), 190–207, https://doi.org/10.1017/9781108966009.010.
[3] David Collier, James Mahoney, and Jason Seawright, "Claiming Too Much: Warnings about Selection Bias," in *Rethinking Social Inquiry: Diverse Tools, Shared Standards* (Lanham: Rowman and Littlefield, 2004), 85–102, https://doi.org/10.1017/S1537592705590157.
[4] Jason Seawright and John Gerring, "Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options," *Political Research Quarterly* 61, no. 2 (2008): 294–308, https://doi.org/10.1177/1065912907313077.

the rate of technological development. It is important to point out here that the relationship between technological growth and globalisation is not always so straightforward. As greater technological discovery also allows greater levels of globalisation. For example, satellites, computers, telephones, and airplanes allow humanity to connect in a way that was never possible before. This creates a feedback loop whereby technological innovation allows mankind to connect, which fuels the sharing of ideas, allowing for more technological progression.[5]

Daniele Archibugi explains three different ways in which technological globalisation happens. The first way is through the exploitation of international technology. It includes those technologies that are produced domestically but are exploited internationally by imitation, licensing, or strategic alliances. The second way is global generation of innovation, where organisations such as multinational corporations and international research teams share information to create new technologies. The last category is the global technological scientific collaborations, where universities, governments, research and development (R&D) organisations work together to develop complex technologies.[6]

Tech globalisation has certain limitations that must be addressed. Certain technologies, such as dual-use technologies or strategic technologies, are restricted by international arms control agreements. Moreover, technologies such as computer chips can be instruments of national power and are a source of national competition. This often leads to technological exploitation, where a less technologically advanced nation is dependent on the sophisticated technology of a more technologically developed country.[7]

Tech Realism

Tech realism or techno realism derives its roots from traditional realist theoretical principles of international anarchy, balance of power, and global hegemony.[8] Whereas the previous school of thoughts like defensive, offensive, or structural realism, were reinterpretations of international politics, techno realism roots itself in the changing nature of technology.[9] The field of science and technology has seen many new emerging technologies like cyber warfare, quantum computing, 3D printing, and artificial intelligence (AI). These technologies have revolutionised the way people live

[5] Daniele Archibugi and Simona Iammarino, "The Globalization of Technological Innovation: Definition and Evidence," *Review of International Political Economy* 9, no. 1 (2002): 98–122, https://doi.org/10.1080/09692290110101126.
[6] Ibid.
[7] Alan Tonelson, "The Perils of Techno-Globalism," *Issues in Science and Technology* 11, no. 4 (Summer 1995): 31–38, http://www.jstor.org/stable/43311451.
[8] Thomas Diez, Ingvild Bode, and Aleksandra Fernandes da Costa, *Key Concepts in International Relations* (London: Sage, 2011), https://doi.org/10.4135/9781446288344.
[9] Steven E. Lobell, "Structural Realism/Offensive and Defensive Realism," *Oxford Research Encyclopedia, International Studies*, December 22, 2017, https://doi.org/10.1093/acrefore/9780190846626.013.304.

their lives, how they interact with the environment, and have had a massive impact on the power dynamics of the international system. Techno-realist attempts to explain the transformative effects of technology on the balance of power.

The theory of techno realism is based on two main assumptions. First, technology is not the root cause of conflict, rather technology is simply an instrument that amplifies human capability, and it has no will of its own. In this sense, techno realism is in line with traditional realist theories which claim that political ideologies play a part in shaping national interests.[10] These ideas can be seen in classical realist literature, such as Morgenthau's, which presumes that ideology is the language of power and helps establish identity of ethnic, political or religious groups. These communities then engage in a competition, which is a power struggle where each side wants to maximise its influence.[11]
Second main assumption relates to the nature of technology as a means of power. This view is shared by Morgenthau, who claimed in 195l that technology changed the relationship between military means and political ends. From a techno realist point of view it is the distribution of technology that determines the balance of power. [12]

Technological realism is different from traditional realism, as it deviates from state centrism and focuses more on technological power and its impact on the security architecture. To traditional realists, technology is simply a tool that states use to achieve their national interests. Tech realism, on the other hand, views technology as capable of reshaping strategic environments, adopting a more technological, deterministic outlook on security. Tech Realism recognises individual groups and corporations along with states as important players in the international security system. Tech companies, new technological innovations, data networks, hostile cyber actors, and computer algorithms carry significance on the geo-political stage. Due to the state approach, traditional realist perceive the military and economy as institutional domains from which states derive their power. However, tech realists claim states derive their power from technological capabilities such as AI, satellite communication, cyber capabilities, and quantum computing.[13]

[10] Isti Marta Sukma, “Techno-Realism: Navigating New Challenges in the Contemporary Role of Technology in Politics,” *Security and Defence Quarterly* 46, no. 2 (2024): 24-46, https://doi.org/10.35467/sdq/188303.
[11] Henrik Bliddal, Casper Sylvest, and Peter Wilson, eds., *Classics of International Relations: Essays in Criticism and Appreciation* (London: Routledge, 2013), 61–68, https://doi.org/10.4324/9780203761472.
[12] Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred. A. Knopf, 1949).
[13] Johan Eriksson and Lindy M. Newlove-Eriksson, "Theorizing Technology and International Relations: Prevailing Perspectives and New Horizons," in *Technology and International Relations: The New Frontier in Global Power*, ed., Giampiero Giacomello, Francesco N. Moro, and Marco Valigi (Cheltenham, UK: Edward Elgar Publishing, 2021), https://doi.org/10.4337/9781788976077.00007.

Mechanism of Tech Globalism across the Technoscape

Technological globalism allows nation states to share ideas to improve connectivity and increase productivity. However, the global community has put some mechanisms in place to regulate the interaction between states and technology. To understand how states cooperate in the technoscape, it is vital to discuss major international institutions and the ways they regulate behaviour in this domain.

International Telecommunication Union (1932)

Originally established in 1865, the International Telecommunication Union (ITU) is responsible for the global telecommunication system,[14] predating the establishment of the United Nations (UN). ITU allocates radio frequencies and establishes technical standards that allow people from different parts of the world to connect. Without international standards, communication would be fragmented, as telephone, internet, and satellites would struggle to interconnect with each other.[15] ITU embodies a common consensus reached by the nation states to establish technical standards. It shows that through common technological standards, states can live in an interconnected global village.

Trade Related Aspects of Intellectual Property Rights (1995)

During the late 1800s and 1900s, intellectual property rights were not regulated by any centralised body. There was only a patchwork of different legal regimes that regulated the intellectual property. For example, Hague and Locarno Agreements regulated industrial designs, the Trademark Law Treaty regulated trademarks. However, this did not end trade disputes, as states were largely free to join any international convention, resulting in conflicts. To fill this lacuna, the World Trade Organisation negotiated an agreement in 1995 called the "Trade Related Aspects of Intellectual Property Rights" (TRIPS). This treaty is responsible for setting global rules for intellectual property, such as trade secrets, trademarks and copyrights. TRIPS is an important enabler for international commerce as it preserves and protects intellectual property, ensuring fair competition which is an essential principle of sustainable trade relations.[16]

[14] Britannica, "International Telecommunication Union," last modified July 11, 2025, https://www.britannica.com/topic/International-Telecommunication-Union.
[15] UN Division for SDGs, "International Telecommunication Union (ITU)," accessed April 30, 2025, https://sdgs.un.org/un-system-sdg-implementation/international-telecommunication-union-itu-24522.
[16] Mehmet Tûba Ongun, "The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), its Implications and Developing Countries," *Journal of Economic Cooperation* 22, no. 2 (2001): 1–30, https://jecd.sesric.org/pdf.php?file=ART01010101-2.pdf.

The Wassenaar Arrangement (1996)

The proliferation of dangerous and harmful weapons has been a key security concern for nation states. To curb the spread of weapons, nation states have formed various international conventions and treaties. The "Wassenaar Arrangement" is a multilateral agreement that is responsible for the restriction of dual-use technology exports. Dual-use is a technology that can be repurposed for military requirements. The agreement came into force in 1996 when the treaty received the approval of 33 states.[17]

Budapest Convention on Cybercrime (2001)

Apart from military technology proliferation, the international community faces threats from the cyber domain, which presents the need for international cooperation against cybercrime and cyber terrorism. The "Budapest Convention" is a binding international agreement that provides a framework for national legislatures against cybercrime.[18] The Budapest Convention is divided in three parts: the first part deals with criminalising a list of actions taken in the cyber domain, the second part deals with procedural law that processes cybercrime and the third part provides a platform international cooperation and justice against cybercrime.[19]

The Budapest Convention is a norm-creating treaty that regulates the cyber activities of individuals. For example, illegal content, unauthorized access, data tampering, systematic interference and misuse of devices. These norms are then implemented through international law enforcement agencies. For example, in 2018, the Interpol with the cooperation of the Indonesian police had arrested an Indonesian-based black hat group named Surabaya. This group was responsible for hacking into thousands of systems across 42 states.[20]

Global Partnership on Artificial Intelligence (2020)

With the increasing traffic in the cyber domain, new digital technologies have emerged; chief among them is AI. The technology of AI is considered disruptive as it completely revolutionises the way people interact with technology. When it comes to AI, commercial and government organisations seek to obtain a competitive edge against their competitors. However, within this competitive framework, 44 states

---

[17] Heinz Gärtner, "The Wassenaar Arrangement (WA): How it is Broken and Needs to be Fixed," *Defense & Security Analysis* 24, no. 1 (2008): 53–60, https://doi.org/10.1080/14751790801903236.
18 Council of Europe, "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols," accessed April 30, 2025, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[19] Helaine Leggat, "A New Look at the Budapest Convention on Cybercrime," *ICTLC*, January 27, 2025, https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en.
[20] Dirga Agung, "The Role of Interpol in the Settlement of Cybercrime Cases under the Budapest Convention on Cybercrimes," *International Journal of Global Community* 5, no. 1 (March 2022): 49–56, https://journal.riksawan.com/index.php/IJGC-RI/article/view/106.

signed the Global Partnership on Artificial Intelligence (GPAI). The purpose of the GPAI agreement is to promote R&D into the responsible use of AI.[21]

Breakthrough technologies, such as OpenAI's ChatGPT and Lethal Autonomous Weapon Systems, have boosted operational and systematic efficiency. However, considerable risks are attached with these technologies. AI can be used by malicious actors, promote inequalities, reinforce discrimination, and displace jobs at a massive scale.[22] To mitigate these threats, international collaboration such as GPAI is needed to shield the global community from the adverse effects of technology.

The US-EU Trade and Technology Council (2021)

The US-EU Trade and Technology Council (TTC) is a recent example of an extra-regional trade organization that facilitates the sharing of technology. It aims to promote common values and interests, strengthen industrial leadership by providing access to the latest technology, and enhance bilateral trade. Some notable projects that the TTC has worked on include AI, semiconductor investment, export controls, the establishment of the Quantum Taskforce, G7 AI code of conduct, and many other similar initiatives[23].

Mechanism of Tech Realism Across the Technoscape

In this section, the research paper will focus on how nation states compete with each other to maximise their own security and pursue their own national interests. To contextualise this phenomenon, this section will discuss the mechanisms and emerging trends in technological competitive behaviour.

Tech Denial

'Tech Denial' is when a state withholds or denies access to a specific technology through export controls, denial of manufacturing equipment and blacklists companies.[24] An example of tech denial policy can be seen in the recent US-China chip war. Washington wishes to block Beijing's access to chip technology to slow down its rapid military and economic modernisation.

---

[21] OECD.AI, "What We Do," *OECD.AI Policy Observatory*, accessed April 30, 2025, https://oecd.ai/en/about/what-we-do.

[22] Huw Roberts, Emmie Hine, Mariarosaria Taddeo, and Luciano Floridi, "Global AI Governance: Barriers and Pathways Forward," *International Affairs* 100, no. 3 (May 2024): 1275–1286, https://doi.org/10.1093/ia/iiae073.

[23] European Commission, "EU-US Trade and Technology Council (2021–2024)," accessed April 30, 2025, https://digital-strategy.ec.europa.eu/en/factpages/eu-us-trade-and-technology-council-2021-2024.

[24] Brad Glosserman, "De-Risking Is Not Enough: Tech Denial Toward China Is Needed," *The Washington Quarterly* 46, no. 4 (October 2023): 103–19, https://doi.org/10.1080/0163660X.2023.2286134.

Semiconductor-based integrated circuits (IC), also called 'chips', can be termed as the basic blueprint of modern technology. A Whitehouse report published in 2022 deemed the semiconductors essential for smart and precision-guided munitions. They are also essential for high-end computer technologies like AI and quantum computing.[25] This makes the semiconductor a lethal dual-use technology, one which can not only boost economic capacity but vastly improve military capabilities.

Due to the critical importance of this technology, both the Washington and Beijing want to ensure a steady supply of chips. The US has encouraged domestic construction of high tech chip production factories called Fabrication Plants or Fabs. To curtail China as a potential competitor in the chip industry, the US has imposed several restrictions such as banning the export of extreme ultraviolet lithography equipment and electronic design automation tools.[26] Below is a brief summary of the series of restrictions the US has imposed on China.

In May 2020, the US Department of Commerce announced a ban on companies utilising American technology to design or produce semiconductors for the Chinese company, Huawei. Due to this, the Taiwan Semiconductor Manufacturing Company stopped accepting Chinese orders.[27] In October 2022, the Biden administration restricted China's access to semiconductor hardware and manufacturing equipment. Additionally, the Bureau had also imposed restrictions on Chinese companies.[28] A year later, in October 2023, (Bureau of Industrial Security) BIS expanded the export controls and imposed restrictions on 13 more Chinese companies.[29] In March 2024, the new set of export controls included chips produced by Nvidia, which are crucial for the development of AI.[30] Most recently, Donald Trump imposed tariffs on US Chinese semiconductor imports, as part of his tariff campaign in his second term in

[25] President's Council of Advisors on Science and Technology, *Report to the President: Revitalizing the U.S. Semiconductor Ecosystem,* report (Washington, D.C.: Executive Office of the President of the United States, 2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/09/PCAST_Semiconductors-Report_Sep2022.pdf.
[26] Yongshin Kim and Sungho Rho, "The US–China Chip War, Economy–Security Nexus, and Asia," *Journal of Chinese Political Science* 29 (February 2024): 433–460, https://doi.org/10.1007/s11366-024-09881-7.
[27] Paul Triolo, "The Evolution of China's Semiconductor Industry under U.S. Export Controls," *American Affairs*, November 20, 2024, https://americanaffairsjournal.org/2024/11/the-evolution-of-chinas-semiconductor-industry-under-u-s-export-controls/.
[28] Reuters, "US Targets China over Semiconductors," updated June 30, 2023, https://www.reuters.com/technology/us-targets-china-over-semiconductors-2023-06-30/.
[29] Covington & Burling LLP, "U.S. Expands October 7, 2022 Export Controls Restrictions on Advanced Computing and Semiconductor Manufacturing Items," October 19, 2023, https://www.cov.com/en/news-and-insights/insights/2023/10/us-expands-october-7-2022-export-controls-restrictions-on-advanced-computing-and-semiconductor-manufacturing-items#:~:text=On%20October%2017%2C%202023%2C%20the,in%20our%20previous%20client%20alert.
[30] "Nvidia, AMD and ASML hit by Trump's Clampdown on AI Chips," *The Times*, accessed April 2025, https://www.thetimes.com/business-money/companies/article/nvidia-faces-55bn-hit-from-trump-clampdown-on-ai-chips-qkl5d03nq.

Oval Office.[31] China, to its end has retaliated in kind, for example, in May 2023 by placing a ban on Micron chips which were used in the construction of national infrastructure projects.[32] Later that year, in August, the Chinese government imposed trade restrictions on the export of germanium and gallium to the US.[33]

Tech Censorship

Tech censorship is the suppression or restrict access to digital technologies, content or social platforms. A key example of tech censorship is US' recent ban on the sale of Huawei and ZTE technologies enacted on the 25th of November, 2022. The Federal Communications Commission (FCC) stated that Huawei, ZTE technologies and other Chinese companies were banned as they were suspected to have espionage devices installed in them.[34]

Huawei is a symbol of Chinese technological modernisation. The company has grown into the second-largest smartphone producer in the world. Huawei is the only telecommunications company offering a 5G network at low prices.[35] This is particularly significant as 5G is the future of wireless telecommunication industry, and is vital for personal consumption and boosting automation and advanced robotics in modern industries.[36] Huawei is outsmarting its competitors in terms of product quality and price. To counter this growth, Huawei has been labelled as a security threat, though, no evidence can be publicly cited of significant vulnerabilities that allow espionage.[37] In addition to allegations of intellectual property theft,[38] the company was accused by

---

[31] Patrick Wingrove and David Lawder, "US Steps up Probes into Pharmaceutical. Chip Imports, Setting Stage for Tariffs," *Reuters*, updated April 15, 2025, https://www.reuters.com/markets/us-initiates-section-232-investigations-into-pharmaceutical-semiconductor-2025-04-14/.

[32] Che Pan, "China Bans Micron Chips for 'Severe Cybersecurity Risks,' Drawing Rebuke from Washington as Tech War Revs Up," *South China Morning Post*, updated May 22, 2023, https://www.scmp.com/tech/tech-war/article/3221331/tech-war-china-says-micron-chips-pose-severe-cybersecurity-risks-effectively-banning-sale-its.

[33] Sarah Godek, "China's Germanium and Gallium Export Restrictions: Consequences for the United States," *Stimson Center*, March 19, 2025, https://www.stimson.org/2025/chinas-germanium-and-gallium-export-restrictions-consequences-for-the-united-states/#:~:text=China's%20new%20ban%20on%20germanium,through%20trade%20via%20third%20countries.

[34] Diane Bartz and Alexandra Alper, "U.S. Bans New Huawei, ZTE Equipment Sales, Citing National Security Risk," *Reuters*, updated December 1, 2022, https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/.

[35] "Can Huawei Survive an Onslaught of Bans and Restrictions Abroad?" *The Economist*, December 15, 2018, https://www.economist.com/business/2018/12/15/can-huawei-survive-an-onslaught-of-bans-and-restrictions-abroad.

[36] Christian de Looper, "What is 5G? Speeds, Coverage, Comparisons, and More," *Digital Trends*, Updated April 25, 2025, https://www.digitaltrends.com/mobile/what-is-5g/.

[37] "The Huawei Way," *Newsweek*, updated March 13, 2010, https://www.newsweek.com/huawei-way-108201.

[38] Harry Cockburn, "Germany 'Planning to Exclude Huawei from New 5G Network' as US Reportedly Investigates Theft Claims," *Independent*, January 17, 2019, https://www.independent.co.uk/news/world/europe/huawei-germany-5g-network-security-china-us-canada-trade-secrets-stolen-meng-wanzhou-a8732661.html.

the Australian intelligence in 2018 of infiltration via Huawei personnel to obtain access codes to foreign networks.[39]

Splinter Net

Splinter Net refers to a contested cyberspace that is regulated by different countries to ensure their digital sovereignty against hostile cyber actors and foreign influence. The boundaries in the Splinter Net consist of the rules and regulations that maintain its digital ecosystem.[40] The concept of the Splinter Net is contrasted by the internet, where all parties can participate from any part of the world. The modern technoscape connectivity resembles more of the internet than Splinter Net. However, recently states have increasingly used restrictions to maintain control of the content that passes through their digital borders.

States predominantly maintain control of the flow of information through internet censorship, which can be manifested in three forms. The first form is internet blackouts, which is the most basic and blunt instrument of information control. During a blackout, the state orders the internet service providers to shut down their access temporarily. States often justify blackouts as a means to counter misinformation. However, blackouts promote internet back doors which are a source of false information.[41] The second form is filtering, where governments and organisations restrict content based on certain rules. These rules could be specific URLs or certain keywords. Content restrictions, while more effective than misinformation, cannot individually analyse the information.[42] To achieve a high level of control, states need to adopt an isolationist approach, which is the third form. In this form, state controls all information that goes in and out of its digital borders, which can be seen in China's "Great Firewall of China." The Chinese firewall keeps malicious and illegal information away through three major ways. Firstly, the firewall blacklists various Internet Protocol (IP) addresses. Secondly, it reduces its Quality of Service, after the data has been filtered from deep packet inspection. In this inspection technique, the data is analysed when being sent over a computer network. And lastly, it filters URLs, where certain

[39] Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, *Huawei, 5G and China as a Security Threat,* report (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019), 8, https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.
[41] Amanda Hetler, "The Splinternet Explained: Everything You Need to Know," *WhatIs.com*, June 7, 2022, TechTarget, accessed July 31, 2025, https://www.techtarget.com/whatis/feature/The-splinternet-explained-Everything-you-need-to-know.
[41] Ronald Deibert et al., eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), 29–54, https://doi.org/10.7551/mitpress/7617.001.0001.
[42] Dainotti, Alberto, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescape. "Analysis of Country-Wide Internet Outages Caused by Censorship." *IEEE/ACM Transactions on Networking* 22, no. 6 (December 2013): 1964–1977. https://doi.org/10.1109/TNET.2013.2291244

keywords, if entered, restrict the access to the website such as Youtube and X (fomer Twitter).[43]

To implement its firewall on a global scale, China introduced a new internet model in 2018 called the Decentralized Internet Infrastructure (DII) and the "New IP" initiative. China aims to set the new technological standards through its representatives in international bodies such as the ITU. China advocates for a multilateral solution with a state-centric approach and claims its internet model is decentralized because it allows states to form their protocols, such as modifying the Digital Object Architecture (DOA). The DOA attributes each information entry with a persistent, unique Internet identifier, just like a Digital Object Identifier (DOI). Internet Identifiers are important as they allow users to recognise the information.

Conversely, the Western model of the internet advocates for a multi-stakeholder solution that includes not only government but also international organisations. Non-profit organisations such as Internet Corporation for Assigned Names and Numbers (ICANN), assign identifiers and domain names. ICANN ensures the security and privacy of domain names. The establishment of such technological standards can create new technological norms that are essential in creating a new digital ecosystems. However, if the Chinese alternative model is successful, it would create a parallel digital ecosystem, which critics believe China is advocating through its Digital Silk Road initiative.[44]

Digital Colonisation

Digital colonisation can be defined as the use of digital technology to dominate and grow at the expense of local firms. Big tech firms often have far greater access to capital and advanced technology, which allows them to acquire data. In digital economies, data is a valuable resource because it can be used for targeted advertising, the development of algorithms, and selling insights derived from data sets.[45]

Data exploitation can happen when tech companies have unfettered access to open markets. For example, in India, Facebook launched the Internet.org which was later renamed to the Free Basics initiative. It provided free access to a limited number of websites, such as job listing websites, Facebook and Wikipedia. It allowed Free Basics to acquire data from millions of internet users, to help create a tech ecosystem where

[43] Jyh-An Lee and Ching-Yi Liu, "Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China," *Minnesota Journal of Law, Science & Technology* 13, no. 1 (2012): 125–151.

[44] Stacie Hoffmann, Dominique Lazanski, and Emily Taylor, "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet," *Journal of Cyber Policy* 5, no. 2 (2020): 239–264, https://doi.org/10.1080/23738871.2020.1805482.

[45] Anirudh Suri, *The Great Tech Game: Shaping Geopolitics and the Destiny of Nations* (Noida, India: Harper Collins India, 2022), 257–69.

Indians were dependent on the Facebook. As a result, local tech companies and services could not compete with Facebook-backed companies in the open market. Consequently, the Indian authorities had banned the Free Basics programme as it violated net neutrality principles.[46]

With such lucrative markets, tech companies often compete for greater access. A good example of this would be the market competition between China's TikTok and Instagram. TikTok, the Chinese social media application, exploded in popularity as the platform had the most engagement: twice as many comments, and brand advertisements as Instagram. This allowed the Chinese companies to collect data on the user's interest and latest trends. This is significant because the more user-data a tech company has, the better its recommendation algorithms become, leading to an increase in user engagement, which in turn means more revenue from advertising companies.[47] The Tiktok hype made the US to view it not only as a competitor in the social media industry but as a national security threat. In March 2023, TikTok's CEO was summoned to the US Congress to address the concerns related to privacy and connection to China via its parent company, ByteDance. The CEO, Mr. Chew, claimed that ByteDance is not under the control of the Chinese government and did not share any data.[48] In January 2025, the US Supreme Court banned TikTok for its failure to divest.

Analysing the Technoscape from the perspective of Tech Realism vs. Tech Globalism

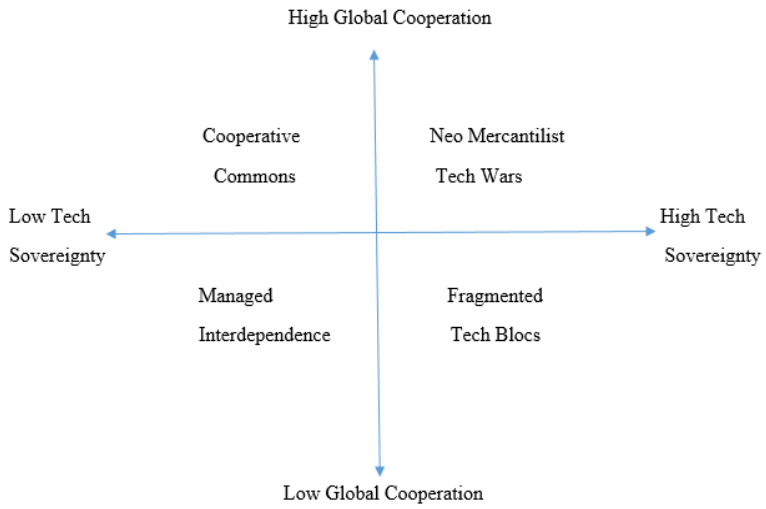
This section will analyse the technoscape from the perspective of Tech Realism and Tech Globalism to determine which theoretical framework explains its nature, with the help of some indicators, the best. The first indicator is the cross-border data flow, which refers to the flow of data from one server to another across different countries. Cross-border data flows are the backbone of the digital economy as they allow states to engage in global trade, communication, and entertainment. In a truly tech global world, there would be no restriction on cross-border data flow. States regulate cross-border data flow to have better access, security, and to protect the civil liberties of their citizens.[49] The second indicator is export control lists, where states regulate the export of products, particularly high-end technology. In an ideal tech global world,

[46] Issie Lapowsky, "India Bans Facebook's Basics App to Support Net Neutrality," *WIRED*, February 8, 2016, https://www.wired.com/2016/02/facebooks-free-basics-app-is-now-banned-in-india/.
[47] Matt G. Southern, "TikTok Dominates Short-Form Content, Instagram Reels Not Far Behind," *Search Engine Journal*, May 30, 2023, https://www.searchenginejournal.com/tiktok-dominates-short-form-content-instagram-reels-not-far-behind/488042/.
[48] David Shepardson, "TikTok CEO to Testify before U.S. Congress over Security Concerns," *Reuters*, updated January 31, 2023, https://www.reuters.com/technology/tiktoks-chief-testify-before-congress-march-wsj-2023-01-30/.
[49] Digital Trade Alliance, "Cross Border Data Flows and Free Trade Agreements," *Factsheet*, January 5, 2024, https://dtalliance.org/2024/01/05/cross-border-data-flows-and-free-trade-agreements/#:~:text=The%20phrase%20%22cross%20border%20data%20flows%22.

there would be export restrictions; however, states enforce export control lists to protect their interests and national security.[50] The last indicator is the digital divide, which refers to the bifurcation in the population between those who have access to the internet, technology, and tech skills and those who don't.[51] The higher the digital divide in a region or globe, the greater the difference in productivity in the global economy. In the interests of the global economy, the digital divide should be minimised, while state interests favour gaining a comparative advantage in the international market.

Measuring these indicators opens four possible distinct possibilities of the nature of technoscape. The diagram below (Figure 1) illustrates these possibilities; the vertical axis measures global tech cooperation, and the horizontal axis tech sovereignty, where states strive to develop their technology.

Figure 1: Scenario Matrix



Source: Info graphic created by author

The first scenario is that Cooperative Commons is governed by a multilateral global organisation that promotes unrestricted data flow, universal tech partnership, and the digital divide is minimal. The second scenario is Neo Mercantilist tech wars, which are fuelled by techno-nationalism. States in this scenario follow protectionist policies that heavily restrict the flow of data, heavily restrict the diffusion of technology, and widen the digital divide. The third scenario is Managed Interdependence, which is a diluted form of Cooperative Commons where states only selectively engage in cooperation

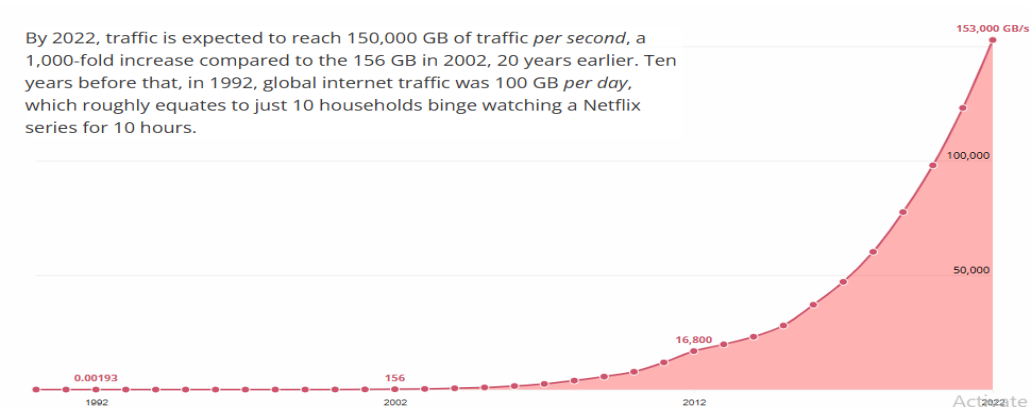
[50] Cornell Research&Innovation, "Export Controls Frequently Asked Questions (FAQ)," accessed July 3, 2025, https://researchservices.cornell.edu/resources/export-controls-frequently-asked-questions-faq.
[51] Jan Van Dijk, *The Digital Divide* (Cambridge: Polity Press, 2020), 12–13.

with organisations. This creates a hybrid model which is mixed tech openness and restriction, where data sharing is conditional to state interests, access to technology is regionally balanced through export controls, and the digital divide is mitigated through targeted programs. The last scenario is Tech Blocs, where states of similar political objectives are organised in Techno Political blocs, creating a similar tech ecosystem. These tech ecosystems will have parallel technological standards, meaning access to data and technology is subject to compatibility. In such cases, states with a weaker or no Techno political blocs will be severely affected by the digital divide.

Cross Border Data Flow:

For a truly tech global world to exist, there needs to be free cross-border data flow, which is unrestricted by government restrictions. Limitations in cross-border data flow may hamper trade and communication, which is the backbone of a global economy. In this regard, data from the World Bank shows that the cross-border data flow increased twenty times between 2007 and 2017.[52] The global volume of data is expected to grow beyond 175 zettabytes in 2025.[53] The figure below shows the exponential rate of increase from 16,800 GB in 2012 to 152,000 GB in 2022. The major traffic was generated by the consumer and commercial industry.

Figure 2: Growth of global internet traffic in the past 30 years

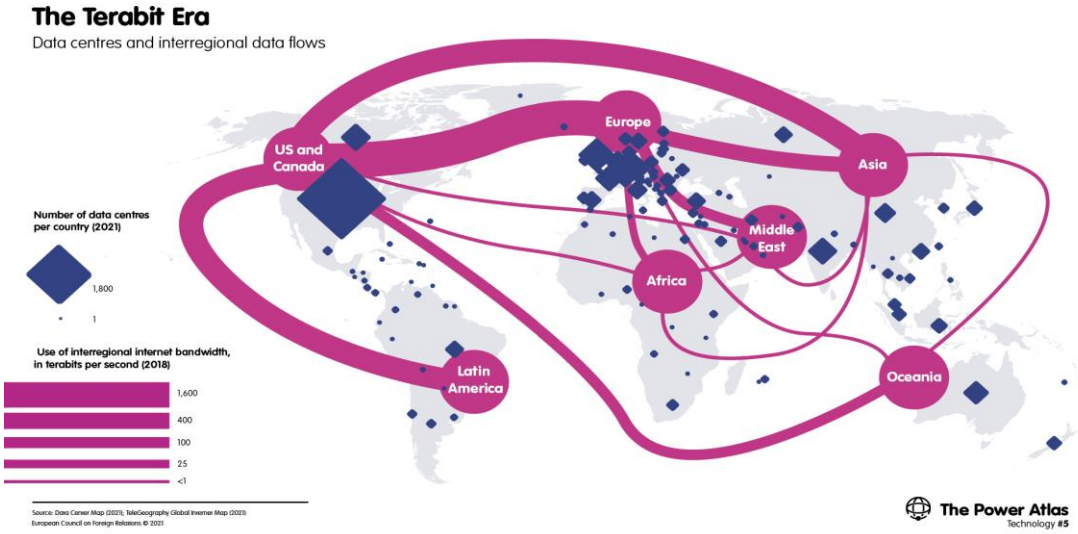


Source: World Bank, "Crossing Borders," World Development Report 2021: Data for Better Lives, accessed July 8, 2025, https://wdr2021.worldbank.org/stories/crossing-borders/

[52] World Bank, *World Development Report 2021: Data for Better Lives*, report(Washington, DC: World Bank, 2021), 237, https://openknowledge.worldbank.org/handle/10986/35218
[53] David Reinsel, John Gantz, and John Rydning, *Data Age 2025: The Digitization of the World, from Edge to Core*, white paper (Framingham, MA: International Data Corporation, November 2018), 3–4, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.

According to a study conducted by the Organisation for Economic Cooperation and Development, a large part of cross-border data flow was produced due to the participation of the emerging economies in the global value chain.[54] The vast majority of the data flow is between the US and Europe, as illustrated by the diagram below, followed by the US to Asia, and lastly by the US to Latin America. The exponential increase in data volume and cross-border flow has led to a USD 2.8 trillion economy in 2014, which could cross USD 11 trillion by 2025.[55]

Figure 3: Data Centre Map 2021



Source: José Ignacio Torreblanca, *Technology*, infographic, in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

The technoscape has undoubtedly seen an increase in the volume of data, but nation-states have also restricted the flow of data to protect digital sovereignty. States protect digital sovereignty to protect their digital resources, data, and infrastructure from exploitation. This includes sensitive information relating to national security and data

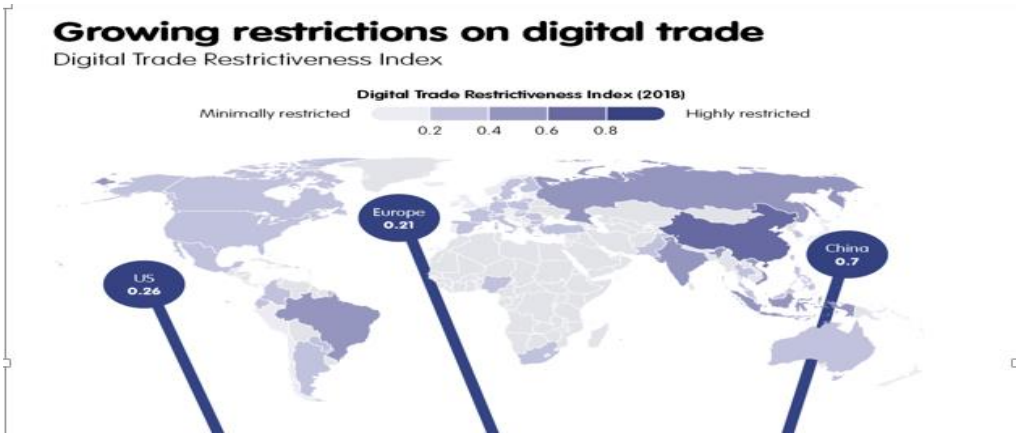
[54] UNCDF Policy Accelerator, *The Role of Cross-Border Data Flows in the Digital Economy,* brief (New York: United Nations Capital Development Fund, July 2022), https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62ed6b995307db59e3e5d2c6/1659726787042/EN-UNCDF-Brief-Cross-Border-Data-Flows-2022.

[55] Joshua Meltzer and Peter Lovelock, "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia," March 20, 2018, Brookings Institution, https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/#_ftn11.

that can be used for economic growth.[56] To gain access to this data, states adopt data localisation policies, where data is stored in a specific geographical location.[57]

Throughout the technoscape, states have adopted different models to balance digital trade with digital security according to their interests. The first model is called "open transfers", where states openly share information. The diagram below (Figure. 4) shows that states like the US have the least restrictive digital trade, which results in a growth in digital services trade. The second model is called "conditional transfers", which balances digital security with digital trade. This model is adopted by European countries, with the most restrictive being France and Germany. The existence of these regulations hampers digital trade in exchange for greater digital control. The third model is the limited transfer model, where the state imposes strict restrictions on cross-border data flow for individuals and companies. This model is particularly prevalent in China, where the government monitors personal data for digital security. This model is least conducive to the growth of digital trade.[58]

Figure 4: Digital Trade



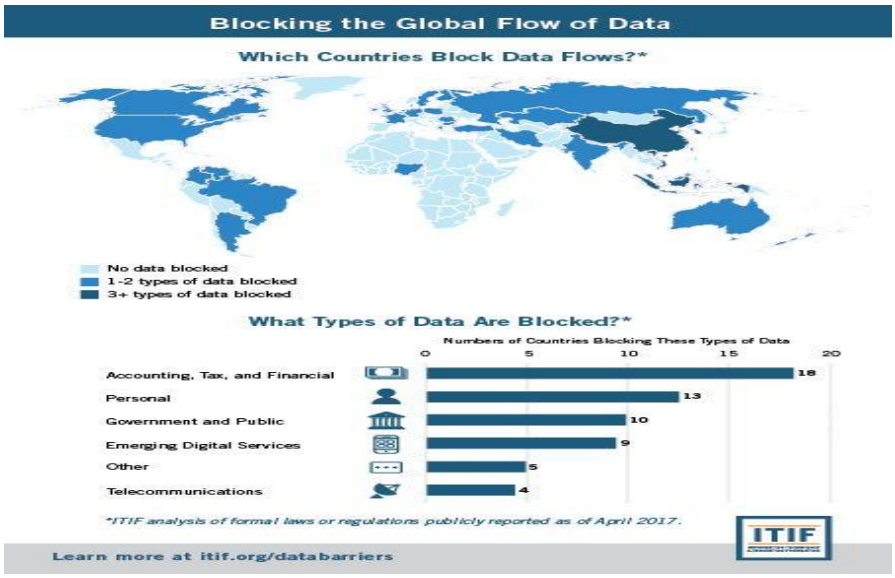
Source: José Ignacio Torreblanca, *Technology*, infographic, in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

The diagram below (Figure. 5) shows categories of data affected by government regulations and restrictions. The data relating to accounting and finance is most affected, which establishes the link between data liberalisation and the growth of digital trade and services. Public and personal data are also under increasing

[56] Min Jiang and Luca Belli, ed, *Digital Sovereignty in the BRICS Countries: A Global South and Emerging Power Alliances Reshaping Digital Governance* (Cambridge: Cambridge University Press, 2024), https://doi.org/10.1017/9781009531085.
[57] Thomas Dewaranu, "Between Cyber Sovereignty and Cross-Border Data Flows," Center for Indonesian Policy Studies, updated April 19, 2022, https://www.cips-indonesia.org/post/opinion-between-cyber-sovereignty-and-cross-border-data-flows.
[58] World Bank, *World Development Report 2021: Data for Better Lives*, report (Washington, DC: World Bank, 2021), https://wdr2021.worldbank.org/stories/crossing-borders/.

surveillance by government agencies, which are motivated by security and political concerns.[59]. While the technoscape has definitively increased its volume of cross-border data flow, there is an increase in government regulations which is affecting the overall growth of the digital economy.

Figure 5: Blocking the Global Flow of Data



Source: Nigel Cory, "Cross-Border Data Flows: Where are the Barriers, and what do they Cost?" *Information Technology and Innovation Foundation*, May 1, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/.

Access to Technology

Access to technology is crucial for increased productivity of a state. In an ideal tech global world, the transfer of technology should be uniform, meaning every state should have an equal chance to take advantage of modern technological systems. However, from the perspective of realpolitik, technology is power that can alter the balance of power, particularly in the case of dual-use technology. The government imposes sanctions to block access to technology to other countries, which may use it as a means to increase their military power.

International institutions like GPAI or US-EU TTC facilitate the transfer of technology. However, in the case of competitive relations like those between the US and China, states impose export controls, among other measures discussed in the previous

[59] Nigel Cory, "Cross-Border Data Flows: Where are the Barriers, and What do they Cost?," *Information Technology & Innovation Foundation*, May 1, 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/.

section. The purpose of these restrictions is to stop the tech diffusion to the adversary states that could threaten the national interests.

The following table shows the policies of restrictions that the Bureau of Industrial Standards (BIS) has imposed from 2022 to 2024. There has been an increasing number of entities (corporations) that have been under export control. These entities are mostly Chinese firms, particularly the tech firms that produce semiconductors. This measure aims to degrade the Chinese production of critical technology, which the US views as a threat to its national security.

Table 1: Export Controls by the BIS.

Year	Description of Export Controls	Entity List Additions	Targeted Entities
2022[60]	Restrictions on Advanced computing and semiconductors	103	Chinese surveillance companies
2023[61]	Semiconductor Manufacturing equipment	96	Chinese companies linked with AI and military tech
2024[62]	Quantum Computing and AI technologies	180	Chinese Chip and Computer Industry

[60] Bureau of Industry and Security, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," *Federal Register* 87, no. 197 (October 13, 2022): 62,186, https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor. Bureau of Industry and Security, "Addition of Entities, Revision and Correction of Entries, and Removal of Entities from the Entity List," *Federal Register* 87, no. 125 (June 30, 2022): 39,446.

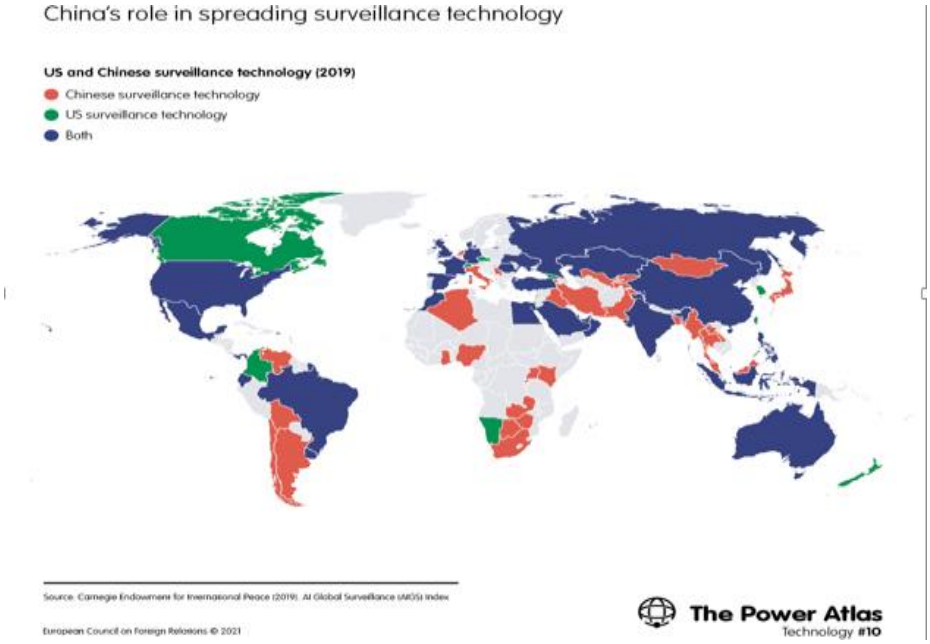
[61] Bureau of Industry and Security, "Additions to the Entity List," *Federal Register* 88, no. 137 (July 19, 2023): 46,314, https://www.federalregister.gov/documents/2023/07/19/2023-15343/additions-to-the-entity-list Bureau of Industry and Security, "Addition of Entities to the Entity List," *Federal Register* 88, no. 195 (October 11, 2023): 69,987, https://www.federalregister.gov/documents/2023/10/11/2023-22536/addition-of-entities-to-the-entity-list.

[62] Bureau of Industry and Security, "Foreign-Produced Direct Product Rule Additions and Refinements to Controls for Advanced Computing Items and Semiconductor Manufacturing Equipment," *Federal Register* 89, no. 234 (December 5, 2024): 85213, https://www.federalregister.gov/documents/2024/12/05/2024-28270/foreign-produced-direct-product-rule-additions-and-refinements-to-controls-for-advanced-computing. WilmerHale, "BIS Issues Sweeping Additional Restrictions on Semiconductors and Advanced Computing; Entity List Designations," *WilmerHale*, December 6, 2024, https://www.wilmerhale.com/en/insights/client-alerts/20241206-bis-issues-sweeping-additional-restrictions-on-semiconductors-and-advanced-computing-entity-list-designations.Gibson Dunn, "International Trade 2024 Year-End Update," *Gibson*

Source: Author's own

The US has imposed export controls to slow down the rate of Chinese military modernisation. However, Western analysts also view Chinese products in Western markets as a potential security threat. Companies like Huawei have been accused of corporate espionage and sharing information with the Chinese government, as part of their military-civilian fusion policy. To counter the threats of Chinese government surveillance, Western governments have placed restrictions on Huawei.[63] The Chinese government, in turn, has also suspected Western products of espionage. This leads to a complicated technoscape, which is illustrated in the map below, showing different areas that are dominated by American and Chinese surveillance technology. This creates artificial tech borders where states, whether for legitimate or perceived security threats, limit technological diffusion across borders.[64]

Figure 6: Surveillance technology in technoscape



Source: José Ignacio Torreblanca, *Technology*, infographic, in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

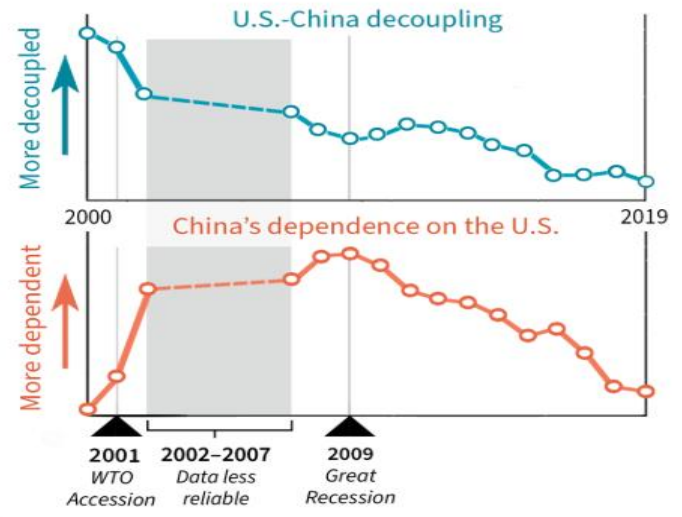
Dunn, December 2024, https://www.gibsondunn.com/international-trade-2024-year-end-update.Chambers & Partners, "Trends and Developments: Export Controls 2024–2025," *Chambers Global Practice Guides: Export Controls*, 2025, https://practiceguides.chambers.com/practice-guides/export-controls-2024/usa/trends-and-developments.

[63] Ferenc Gaál, "China's Surveillance Tech: Western Bans, Global Growth," *Deutsche Welle*, March 29, 2023, https://www.dw.com/en/western-countries-are-banning-chinese-tech-why-is-it-still-spreading/a-65106709.

[67] José Ignacio Torreblanca, "Technology," European Council on Foreign Relations, accessed July 8, 2025, https://ecfr.eu/special/power-atlas/technology/.

These artificial tech boundaries have led to the phenomenon known as Tech Decoupling, where states reduce technological interdependence, for political or security reasons. The US-China technological competition has led to technological decoupling, as illustrated in Figure number 7. In 2000, China was largely decoupled from American technology due to its isolationist policies. In 2001, China began to integrate into the global technoscape following its accession to the World Trade Organisation. In 2009, as the graph below illustrates, Chinese dependence on US technology had reached its peak. After the global recession, Chinese R&D began developing its digital technology, like Alipay or WeChat. The pace of decoupling increased significantly after 2018, when the US imposed sanctions on China. [65]

Figure 7: US-China tech decoupling and dependence



Source: Pengfei Han, Wei Jiang, and Danqing Mei, "Mapping U.S.–China Technology Decoupling and Dependence," *China Briefs*, Stanford Center on China's Economy and Institutions, accessed July 8, 2025, https://sccei.fsi.stanford.edu/china-briefs/mapping-us-china-technology-decoupling-and-dependence.

However, some scholars debate whether the US and China are decoupling or engaging in technological bifurcation. Technological bifurcation means that tech ecosystems are separating into separate systems that coexist, having their unique platforms, supply chains, and technological standards, creating a sphere of influence.[66] A good example

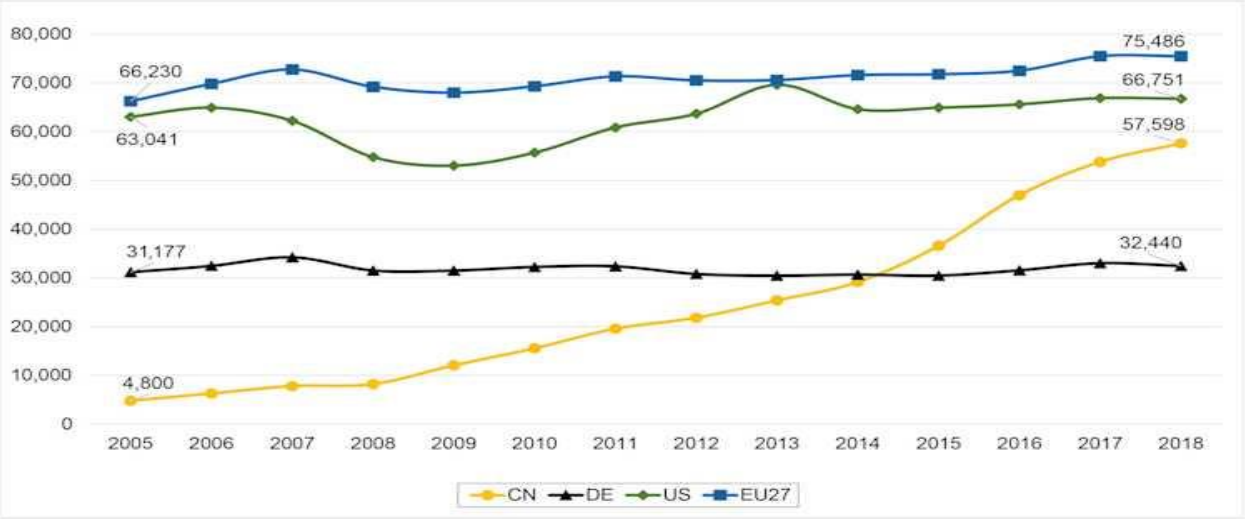
[65] Pengfei Han, Wei Jiang, and Danqing Mei, "Mapping U.S.-China Technology Decoupling and Dependence," Stanford Center on China's Economy and Institutions, updated April 5, 2024, https://dx.doi.org/10.2139/ssrn.3779452.

[66] Alicia García-Herrero, "China and the US Might Not Be Decoupling but their Technologies are Bifurcating," *Bruegel*, May 16, 2023, https://www.bruegel.org/newsletter/china-and-us-might-not-be-decoupling-their-technologies-are-bifurcating.

of this would be the American Global Positioning System (GPS) and the Chinese Baidu system, each providing a competing global navigation system.

The Technological competition centres on the expansion of the technological sphere of influence. Both China and the US are looking to export their technological standards and platforms. To achieve this, states need to produce the latest technology at a faster rate than their competitors. Those companies that succeed in getting their product first in the market have the advantage of establishing platforms and setting the technological standards. Patents are a good metric to estimate the technological development of a state. China's patents have seen a dramatic increase from 4,800 patents in 2005 to 57,598 in 2018. China is currently leading in the scientific publications in the fields of Industrial Biotech, Microelectronics, Bio-Economy, Renewable Energy, and New Materials. Despite China's impressive performance, the US still leads the technological world with 75,486 patents, followed by Europe with 66,751 patents.[67]

Figure 8: Number of Patents.



Source: Margot Schüller and Yun Schüler-Zhou, "United States–China Decoupling: Time for European Tech Sovereignty," *GIGA Focus Asia*, no. 7 (Hamburg: German Institute for Global and Area Studies, 2020), accessed July 8, 2025, https://www.giga-hamburg.de/en/publications/giga-focus/united-states-china-decoupling-time-for-european-tech-sovereignty.

The number of Patents alone does not determine technological performance, as products need to be sold in the market for states to expand their technological

[67] Margot Schüller and Yun Schüler-Zhou, "United States–China Decoupling: Time for European Tech Sovereignty," *GIGA Focus Asia*, no. 7 (2020), https://nbn-resolving.org/urn:nbn:de:0168-ssoar-71026-4.

influence. To measure this influence, the Organisation for Economic Co-operation and Development (OECD) uses high-tech exports, as products are R&D intensive. In 2018, China had 21 percent of the global high-tech export market, while the US had 32 percent.[68] Though the Chinese lead the tech industry in the number of patents, they are behind the high-tech export industry, as shown in the table below.

Table 2: High-Tech Exports

Technology Field	China	United States	EU27
Industrial Biotech	4	1	3
Nanotechnology	4	1	2
Microelectronics	2	3	4
Photonics	4	3	2
New Materials	4	3	2
Advanced Production	5	3	1
Bio Economy	4	1	2
Renewable Energy	5	3	1

Source: Margot Schüller and Yun Schüler-Zhou, "United States–China Decoupling: Time for European Tech Sovereignty," *GIGA Focus Asia*, no. 7 (Hamburg: German Institute for Global and Area Studies, December 2020), https://www.giga-hamburg.de/en/publications/giga-focus/united-states-china-decoupling-time-for-european-tech-sovereignty.

The tech competition between Washington and Beijing has started to fragment the liberal technological global order. Technology has faced restrictions in the form of tech denial and censorship, due to actual or perceived security threats. While the existence

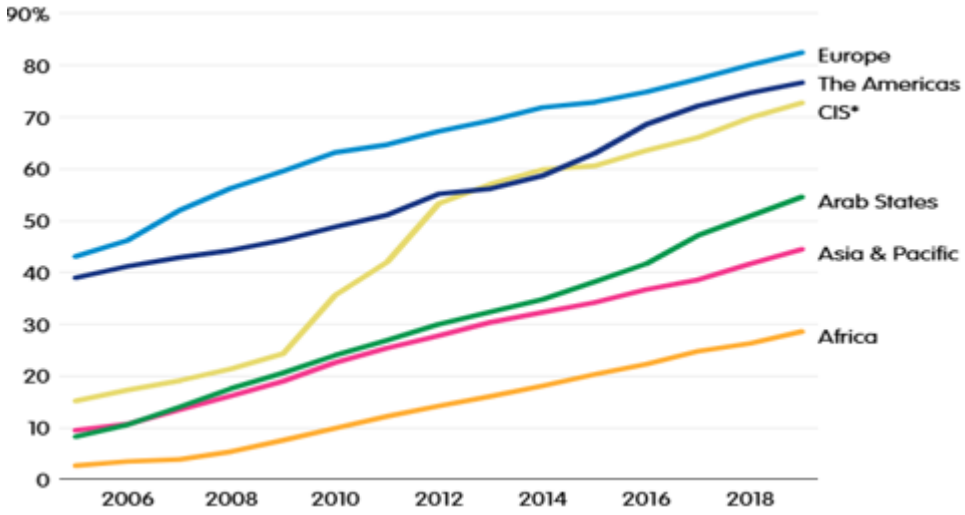
[68] Alexander B. Hammer and Shahid Yusuf, *"*Is China in a High-Tech, Low-Productivity Trap?*"* (paper, U.S. International Trade Commission, Washington, 2020), https://www.usitc.gov/publications/332/working_papers/2020-07_chinainnovationwphammeryusuf.pdf.

of technological blocs seems unlikely short term, there are early signs of a technological bifurcated future.

Digital Divide

Digital divide is the disparity in the population between those who have access to internet and those who do not. In an ideal tech global world, the digital divide needs to be as minimal as possible. To measure the digital divide, a key metric is access to the internet and its disparity in distribution.[69]

Figure 9: Percentage of population using the Internet



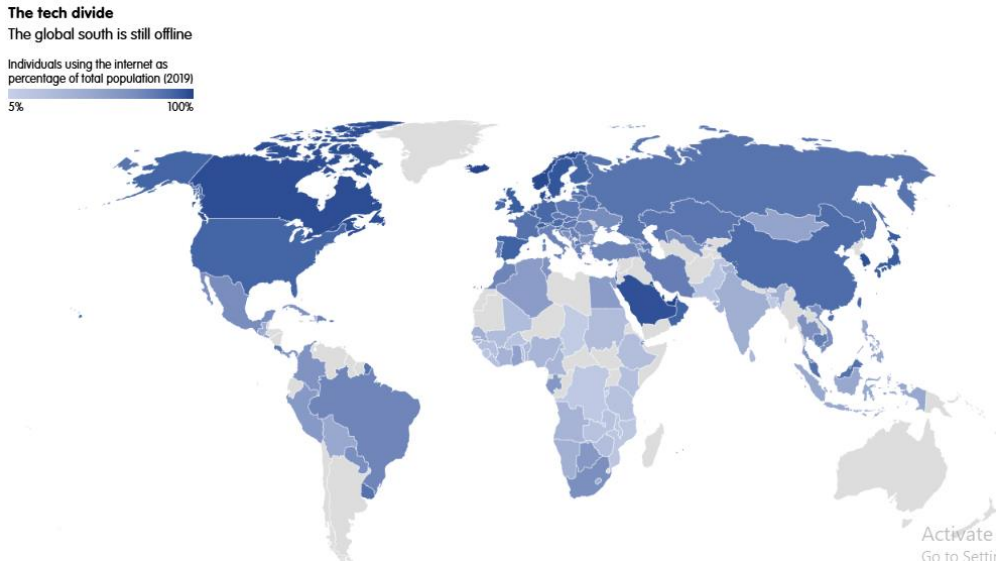
Source: José Ignacio Torreblanca, *Technology*, infographic, in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

There has been a general upward increase in the total number of people connected to the internet all across the globe; however, the disparity between regions has increased. In 2006, regions like Asia and Africa had a low internet connectivity rate of less than 10 percent. In 2018, the internet connectivity had grown to 28 percent in Africa, about 42 percent in Asia, and Arab 53 percent. The regions with the highest connectivity are the US, with 78 percent, and Europe, with 82 percent. These figures clearly show a significant disparity in internet connectivity between Western countries and developing countries, particularly in Africa. A report by the United Nations-Habitat in 2021 pointed out several reasons for the disparity of internet connectivity between developed and developing states. The report pointed out the difference between rural and urban populations. In developing states, 17 percent had no internet connectivity, and 19 percent had 2G connectivity. On the other hand, 72 percent of urban areas have internet access. Another key difference is access to the internet for the young population. The youth in developing countries comprises 66 percent of the population,

[69] UN-Habitat, *Assessing the Digital Divide* (Nairobi: United Nations Human Settlements Programme, 2021), https://unhabitat.org/sites/default/files/2021/11/assessing_the_digital_divide.pdf.

it is 98 percent for the developed countries. Lastly, there is a pronounced difference in internet access across genders. Fifty-five percent of males have access to the internet in comparison to 48 percent of females, which accounts for 327 million fewer women.[70]

Figure 10: Tech Divide



Source: José Ignacio Torreblanca, *Technology*, infographic, in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

The map above illustrates the disparity in internet connectivity across regions. As expected, the areas of the global north are generally well-connected. For example, Canada has 96.5 percent, Norway 98 percent, and the USA 89.4 percent connectivity. The Global South generally has lower internet connectivity, such as India has 41 percent and Nigeria has 33.6 percent connectivity. Some Global South states have abysmal connectivity rates, such as Chad with 9.8 percent and the Democratic Republic of Congo with 12.5 percent. Though among the Global South, there are exceptions, states with high connectivity like China with 86.5 percent and Saudi Arabia with 95.7 percent.[71] The techno graphic analysis indicates a huge disparity between the Global North and the Global South countries. The lack of availability of internet access creates unequal opportunities, as technology cannot function without proper connectivity.

Conclusion

The technoscape is a complex web of cooperation and conflict which coexist with each other. In terms of cooperation, tech globalism has facilitated progress by providing a

[70] Ibid.
[71] José Ignacio Torreblanca, "Technology," in *The Power Atlas*, European Council on Foreign Relations, accessed July 31, 2025, https://ecfr.eu/special/power-atlas/technology/.

framework and international institutions. For example organisations like ITU facilitate international communication by allocating radio frequencies. Another example is TRIPS which protects intellectual property that is vital for international commerce. States often cooperate with each other to share new technological ideas through platforms like Global Partnership on Artificial intelligence. These institutions and multilateral cooperations develop trust and spread technical knowledge that make international trade possible. Apart from promoting international trade, the international community has formed agreements that regulates state behavior. For example the Wassenaar Arrangement restricts the export of dual use technologies and the Budapest Convention provides a framework against cybercrime.

While the international institutions and multilateral agreements are a critical part of the architecture of the modern technoscape, political realism has fractured connectivity between states. States operating under the paradigm of techno-realism view technology as an instrument of power that must be controlled. They resort to several strategies, including tech denial that involves restricted supply of raw materials or critical components. If the production of technology cannot be curbed, states can restrict access to its content, limiting its influence. These measures create tecno-ecosystems that are separate from each other, as in the case of Splinter Net where access to cyberspace is restricted. These measures enact artificial technological boundaries which retard the speed of diffusion of ideas and technology.

In conclusion, the global technoscape has seen a massive increase in the volume of cross-border data flow. The internet traffic has increased despite government restrictions, particularly for financial information. However, there is a great disparity in internet connectivity between the Global North and the Global South, which clearly shows a digital divide. This digital divide affects the growth digital economy more than government restrictions. In terms of the transfer of technology, low-end technology is transferred with few restrictions. However, in the case of high-end technology, particularly dual-use technology, the technoscape has seen an increase in restrictions. The technoscape has also seen an increase in tech polarisation, where the world is being increasingly divided by technological services and products. Though there is little evidence of tech blocs due to the unrealistic nature of tech decoupling, technological bifurcation is becoming an emerging reality. This means the technoscape is oscillating between managed interdependence to tech blocs.

ABOUT THE AUTHOR

Syed Ahmed Ali *is a Research Assistant at the Centre for Aerospace & Security Studies, Islamabad. Earlier, he worked with the Islamabad Policy Research Institute (IPRI) and taught at National Defence University as visiting faculty. His research interests include emerging technologies, particularly cyber security and Artificial Intelligence. His insights are frequently published in leading newspapers such as* 'Express Tribune' *and* 'The News International'. *He completed his MPhil in Strategic Studies from the National Defence University and his undergrad from SZABIST University in International Relations.*

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security

Strategic Foresight

CASS www.casstt.com
CENTRE FOR AEROSPACE & SECURITY STUDIES, ISLAMABAD
Independence | Analytical Rigour | Foresight

Old Airport Road, Islamabad, Pakistan
+92 051 5405011
cass.thinkers@casstt.com
www.casstt.com
@CassThinkers
Centre for Aerospace & Security Studies
cassthinkers
cass.thinkers