US-CHINA RIVALRY: CONSTRUCTING VIRTUAL BORDERS IN CYBERSPACE THROUGH WAR NARRATIVES

Dibakar De[1], Naga Laxmi M Raman[2], Sitakanta Mishra[3]
Amity University Noida, India, Pandit Deendayal Petroleum University India

Abstract:

Cyberspace has redefined national borders, prompting a rethink of traditional concepts of territoriality. In this digital realm, nations can leverage technological advancements to expand their influence beyond physical borders. This article begins by discussing the rapid emergence of narratives in cyberspace, before exploring the concept of territoriality in a virtual landscape and the roles played by both state and non-state actors. The rest of the article explores a range of aspects, including covert operations, fintech policies, divisions in emerging technologies such as AI, tech diplomacy, export control, and space-based digital infrastructure, to establish the notion of ideological and political fragmentation within cyberspace. Finally, it discusses the various strategies employed by the US, China and other actors to exploit the fragmentation of cyberspace for their own national benefit.

Keywords: Cyberspace, Virtual Borders, Digital Revolution, Public Diplomacy, Great Powers, U.S., China

Titulo en Español: *Rivalidad entre EE. UU. y China: Construcción de fronteras virtuales en el ciberespacio a través de la guerra de narrativas*.

Resumen:

El ciberespacio ha redefinido las fronteras nacionales, lo que ha llevado a replantearse los conceptos tradicionales de territorialidad. En este ámbito digital, las naciones pueden aprovechar los avances tecnológicos para ampliar su influencia más allá de las fronteras físicas. Este artículo comienza analizando la rápida aparición de narrativas en el ciberespacio, antes de explorar el concepto de territorialidad en un paisaje virtual y las funciones que desempeñan tanto los actores estatales como los no estatales. El resto del artículo explora una serie de aspectos, entre los que se incluyen las operaciones encubiertas, las políticas de tecnología financiera, las divisiones en tecnologías emergentes como la inteligencia artificial, la diplomacia tecnológica, el control de las exportaciones, y la infraestructura digital espacial, con el fin de establecer la noción de fragmentación ideológica y política dentro del ciberespacio. Por último, analiza las diversas estrategias empleadas por Estados Unidos, China y otros actores para explotar la fragmentación del ciberespacio en beneficio de sus propios intereses nacionales.

Palabras Clave: *Ciberespacio, fronteras virtuales, revolución digital, diplomacia pública, grandes potencias, EE. UU., China,*

[1]Dibakar De is a Doctoral Scholar, Amity Institute of International Studies, Amity University, Noida, Uttar Pradesh, India. E-mail:<dibakar.de@s.amity.edu>
[2] Naga Laxmi M Raman is Director & Head of Institute, Amity Institute of International Studies Amity University Uttar Pradesh, Noida, Uttar Pradesh, India. Email:<nlraman@amity.edu>
[3] Sitakanta Mishra is an Associate Professor, Social Sciences, School of Liberal Studies, Pandit Deendayal Petroleum University, Gujarat, India. Email: <Sitakanta.Mishra@sls.pdpu.ac.in>
DOI: http://dx.doi.org/10.31439/UNISCI-239

1. Introduction

Both the unifying and dividing elements of our modern society are embodied in cyberspace, which is frequently hailed as the ultimate frontier for globalisation. Being a digital construct, it crosses conventional geographic borders and makes it possible for people to exchange information, culture, and goods on a global scale and at a speed never before possible. A borderless world, where the exchange of ideas and commercial activity is unhindered by the physical limitations that formerly characterised international interactions, is supposedly fostered by this connectivity.[4] This deterritorialized aspect of cyberspace, however, also reinforces the forces of fragmentation, disruptive nationalism, and state sovereignty, resulting in a paradox whereby the same medium that promises global integration also reasserts boundaries and exacerbates divisions. According to the theory of a borderless world, the digital world may surpass the boundaries of the real world and establish a global village where political, cultural, and economic divisions are dissolved.[5] This vision aligns with the broader goals of globalisation, which seeks to integrate economies, societies, and cultures into a cohesive global system. Examples of this unifying potential are social media platforms like Facebook, X (formerly Twitter), and TikTok, which enable users from diverse cultural and national backgrounds to interact and share content instantaneously, thereby fostering a sense of global community.

E-commerce giants like Amazon and Alibaba epitomise the dissolution of economic borders, allowing consumers to access goods and services from around the world with the click of a button. However, the reality of cyberspace is far more complex. Rather than erasing borders, cyberspace often reinforces them, manifesting in the phenomenon of digital nationalism.[6] States increasingly assert their sovereignty over the digital domain through mechanisms such as internet censorship, data localisation laws, and the creation of national firewalls. China's Great Firewall, for instance, effectively creates a digital border that controls the flow of information into and out of the country, thereby preserving the state's control over its domestic cyberspace. Similarly, Russia's "Sovereign Internet" law, enacted in 2019, empowers the government to isolate the Russian internet from the global web, ensuring that Russian cyberspace operates independently of foreign influence.[7] Moreover, the rise of cyber warfare and the use of cyberspace for espionage and propaganda further complicates the narrative of a borderless world. Cyberspace has become a battleground for state and non-state actors alike, where traditional notions of territorial sovereignty are reconfigured in the digital age. The 2016 US presidential election, marred by allegations of Russian interference through cyber means, underscores the potential of cyberspace to disrupt national sovereignty and influence political processes across borders. Similarly, the use of cyberspace by extremist groups to spread propaganda and recruit members across national boundaries demonstrates how digital connectivity can foster fragmentation rather than unity.

In addition to state actions, the corporate control of cyberspace also challenges the idea of a borderless world. The dominance of a few multinational technology corporations, often referred to as Big Tech or Tech Giants, creates a form of digital oligopoly that centralises control over vast strips of the internet. Companies like Google, Apple, and Facebook exert

[4] Fu, Xiaolan, Avenyo, Elvis, & Ghauri, Pervez: "Digital platforms and development: a survey of the literature". *Innovation and Development*, vol. 11, nº 2–3 (September 2021), pp. 303–321. https://doi.org/10.1080/2157930X.2021.1975361

[5] Dalton, Yasmin: "Has globalisation created a "borderless world" in the post-Cold War era?", June 2019.

[6] Lambach, Daniel: "The Territorialization of Cyberspace". *International Studies Review*, vol. 22, nº 3 (May 2019), pp. 482–506. https://doi.org/10.1093/isr/viz022.

[7] "Russia: Growing Internet Isolation, Control, Censorship", Human Rights Watch, 18 June 2020. https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

significant influence over the global flow of information, raising concerns about digital imperialism where the internet, rather than being a democratising force, becomes a tool for economic and cultural dominance by a few powerful entities.[8] Nvidia, which specialises in advanced computing technologies, including artificial intelligence (AI), graphics processing units (GPUs), and virtual environments, are uniquely positioned to influence and shape narratives even further.[9] This centralisation of power not only undermines the egalitarian potential of cyberspace but also creates new forms of digital exclusion, where access to information and digital resources is unevenly distributed across the globe. The paradoxical nature of cyberspace as both a unifying and divisive force is further exemplified by the concept of "filter bubbles" and "echo chambers."[10] While the internet provides access to a vast array of perspectives and information, algorithms designed to personalise content often result in users being exposed primarily to information that aligns with their existing beliefs. This opens a door to certain questions being welcomed: how does the build-up of different narratives and ideological factions within cyberspace end up fragmenting the international community as a collective? A follow up question to this is, how do these fragmentations and divisions give rise to proxy borders even more? A slight shift away from the philosophical aspect of the cyber domain would also allow us to delve into the more physically observable area of the topic—how countries have begun leveraging digital interconnectivity to establish virtual borders through the exploitation of interdependence.

2. Birth of new borders through narratives

A narrative is a loosely used term which serves the purpose of describing a wide range of phenomena broadly related to storytelling and communications.[11] It is also about time, creating a logical sequence between the past, present and future through which a collective sense of space and a sense of place is established.[12] This study will analyse two types of state-actors to fulfil the research objectives: great powers and regions (lesser countries cannot leverage adequate influence unless they come together as a collective region). The other type of actors analysed are non-state actors such as big tech corporations, NGOs and hacktivist groups.

2.1 Cyberspace, State-Actors and Territoriality

Governments use the internet to construct narratives in order to control public opinion, change public perceptions, and advance their geopolitical objectives. These stories are created and shared using a range of internet outlets, news websites, social media, and official government channels. States can design and project certain narratives that correspond with their national interests, cultural values, and strategic aims by managing the flow of information in cyberspace[13]. State authority can be asserted both domestically and internationally through the process of narrative construction in cyberspace. Since it creates a sense of identity, belonging,

[8] Shaleen Khanal, Hongzhou Zhang, Araz Taeihagh: "Why and how is the power of Big Tech increasing in the policy process? The case of generative AI", *Policy and Society* (March 2024), pp. 1-18, at https://doi.org/10.1093/polsoc/puae012

[9] Varshney, Gaurang: "The Dark Horse in the Era of AI: The Nvidia Story", *Economic Times,* 21 June 2024, at https://brandequity.economictimes.indiatimes.com/news/digital/the-dark-horse-in-the-era-of-ai-the-nvidia-story/111168499

[10] Bruns, Alex: "Filter bubble". *Internet Policy Review*, vol. 8, nº 4 (November 2019), https://doi.org/10.14763/2019.4.1426

[11] Liveley, Genevieve: "Stories of cyber security combined report". *Research Institute for Sociotechnical Cyber Security* (February 2022), pp. 4.

[12] Miskimmon, Alister, O'Loughlin, Ben & Roselle, Laura (eds.) (2017), *Forging the World. Strategic Narratives and International Relations*, University of Michigan Press.

[13] Barrinha, Andre, & Turner, Rebecca: "Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India", *Contemporary Security Policy*, vol. 45*, nº* 1 (October 2023), pp. 72–109.at https://doi.org/10.1080/13523260.2023.2266906

and even exclusion within particular digital communities, this strategic communication can in fact lead to the emergence of virtual boundaries and sentiments of territoriality in cyberspace.

There are various actors that use a variety of methods to achieve the dissemination of narratives in cyberspace, each with a distinct audience and set of goals. State actors providing some of the greatest demonstrable risks, are considered to be the most powerful actors in cyberspace and have the capacity to engage in divisive behaviour, promote policies that fragment the internet into multiple sub-spaces and create intangible as well as tangible barriers.[14] Propaganda and Information Warfare to influence public opinion both within their own borders and internationally, are amongst the most widely utilised tools by governments. This manifests itself in cyberspace as fake news, state-sponsored content, and misinformation efforts that try to sway people's opinions and provide a positive picture. All of the current great powers including the U.S., China and Russia, have consistently been leveraging the far-reaching connectivity offered by cyberspace to generate divisive narratives that ultimately lead to the establishment of various barriers and borders throughout the world.

2.2 China's Strategy

China's strategic narrative-building initiatives have allowed it to become a major player in shaping cyberspace. Through the use of technology for surveillance, the manipulation of digital platforms, and the propagation of state-sponsored narratives, China has created robust virtual borders that bolster its territorial claims in cyberspace. By isolating China's domestic internet from external influences and advancing a unified and controlled narrative domestically and, increasingly, internationally, these activities foster a sense of digital sovereignty. One of the most prominent aspects of China's cyberspace strategy is the creation and maintenance of the Great Firewall, a massive censorship apparatus that filters and controls access to foreign websites and content. This has allowed China to construct virtual borders that keep out external influences while tightly regulating the information its citizens can access.[15]
The Great Firewall promotes homegrown alternatives like WeChat, Weibo, and Baidu while blocking international websites like Google, Facebook, Twitter, and YouTube.[16] Due to the tight government control these platforms enjoy, only official stories are allowed to spread over China's internet. China's digital ecosystem and the rest of the world are virtually divided by this exclusive access to the global internet[17] (Ibid.). Chinese internet users are cut off from outside viewpoints, and their online realm is dominated by stories that are specific to China. China also promotes a type of digital territoriality by barring foreign platforms, restricting Chinese internet users to state-approved digital areas and making it impossible for outsiders to enter this tightly controlled environment *(Please refer to Table 1 for a list of policies aimed at reinforcing internet sovereignty)*.

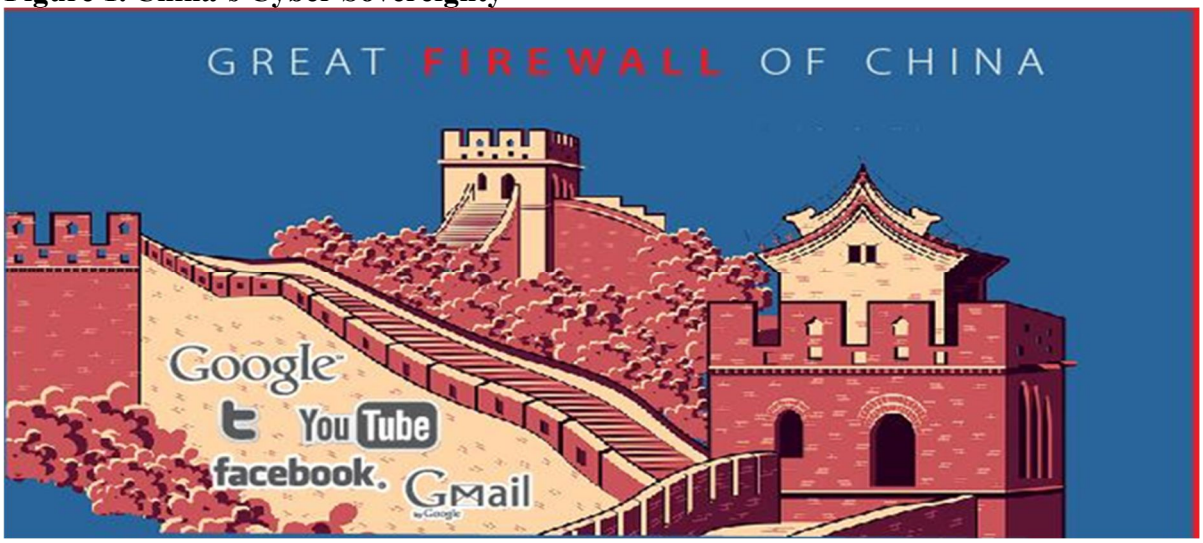
The CCP's practice of heavy narrative control and censorship support a type of nationalism in which Chinese people are exposed to content that has been carefully chosen to highlight the virtues of China and its leadership.[18] This narrative construction is quite exclusive; it promotes cohesiveness among the group while portraying outsiders—especially those from

[14] Ramen, Aishwarya: "States' use of non-state actors in Cyberspace", ORF Expert Speak Young Voices, August 2023, at https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace.
[15] Shen, Fei: "Great Firewall of China", *Encyclopaedia of Social Media and Politics,* vol. 2. (January 2014), pp. 599-602.
[16] Green, Kieran, Sprott, Andrew, Francis, Ed, Lafferty, Brian, Hartley Wise, Henry, Molly, Faerber, Grace, and Miller, Frank: "Censorship practices of the People's Republic of China", Centre for Intelligence Research and Analysis, Exovera, 20 February 2024, pp. 56, at https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf
[17] *Ibid*., pp. 02.
[18] *Ibid*., pp. 45.

the West—as enemies or threats. As a result, Chinese citizens perceive their digital world as unique and superior to the chaotic, uncontrolled character of the global internet, strengthening the sense of territoriality in cyberspace. China is attempting to establish supremacy in the digital and diplomatic domains, as seen by its assertive online posture, which is sometimes referred to as "Wolf Warrior Diplomacy." Chinese internet users and diplomats, occasionally enlisted by the government, participate in online debates, defending China's policies and criticising other countries' governments or media outlets, especially on social media sites like Reddit or Twitter, especially in the matters of how it handled Covid-19, Hong Kong, Taiwan, Xinjiang Crisis etc.[19]

As a result of this vigorous defence of China's image on international platforms, Chinese users feel compelled to defend their nation's digital sovereignty. This feeds into a sense of territoriality. They wage virtual wars to defend China's narrative, dividing Chinese internet users from international populations.

Figure 1. China's Cyber Sovereignty



Source: China's Great Firewall: Business Implications

The way in which users protect their "digital homeland" from alleged outside attacks is reminiscent of old ideas of territoriality.

The CCP also heavily engages in promoting a dominant narrative by tightly controlling domestic online discourses to ensure that only pro-government narratives thrive. For example, post COVID-19 crackdowns in the nation, the Chinese government had also issued a mandate which allowed for the arrest of anybody who was caught "liking" certain anti-China posts online, without mentioning exactly which type of content was deemed illegal.[20] The CCP seems to have created a single, prevailing narrative of Chinese national pride, unity, and prosperity under party rule through its control over online content. As a result, opposing ideas are silenced and a feeling of digital territoriality is promoted, marginalising criticism and fostering nationalist mentality.

China has been involved in vehement attempts at shaping international narratives, especially in cyberspace, by heavily utilising state-run media channels like Xinhua, CGTN, and Global Times. These media sources create information for global audiences in a variety of languages, promoting a pro-China narrative while refuting narratives from Western media that

[19] Liu, Kerry: "China's Wolf Warrior Diplomacy (Narrative): Development, Causes, and Political Effects", *Diplomatica*. vol. 6, nº 1 (April 2024), pp. 71-99.
[20] He, Laura: "China's New Internet Rule Punishes 'Liking' Posts", *CNN*, 30 November 2022.

criticise China's policies.[21] Global virtual borders have been strengthened as a result of China's efforts to have its cyber sovereignty doctrine—which holds that each nation has the right to manage its own internet free from outside intervention—accepted internationally. This theory advocates for autonomous nation-state management of cyberspace, similar to China's behaviour within the Great Firewall. China has been trying with great vigour, to export its cyberspace governance model under this doctrine, providing authoritarian governments with a guide on how to keep control over the internet while staying in power. Countries like Vietnam, Saudi Arabia, and Iran are following suit, perceiving China's strategy as an effective means of stifling opposition and advancing official narratives.[22]

A glaring example of Chinese attempts and fragmenting the internet through weaponisation of narratives is the "50 Cent Party (五毛党, *wǔmáo dǎng*)". By influencing online conversation, stifling dissent, and cultivating an ecosystem of information control that warps international digital connections, it is a state-sponsored online propaganda force has greatly contributed to the fragmentation of cyberspace. In order to influence online debates in support of the Chinese Communist Party (CCP), state-sponsored internet commentators are referred to as the "50 Cent Party" and are supposedly paid 0.50 yuan per post. Researchers estimate that these agents strategically flood cyberspace with pro-CCP narratives and silence dissenting voices, producing millions of posts annually. Digital spaces are further divided by the propagation of nationalist speech, which heightens animosity against Western institutions, the United States, and liberal democratic norms.[23]

China assists nations cooperating with its Belt and Road Initiative in creating virtual borders to guarantee that their governments have control over internet material, in addition to helping these nations develop their digital infrastructure. These imaginary borders, which replicate China's own, support narratives that are favourable to China while bolstering authoritarian authority. As governments in recipient nations are likely to accept China's narrative and bar Western criticism from their cyberspaces, China obtains power in these digital domains in exchange. Another example of the Chinese leadership working towards establishing further digital divide in the current world order is by providing surveillance technologies to international governments. For example, in order to address the city's crime issues, Kampala police in Uganda purchased $126 million worth of monitoring equipment from Huawei in 2019. But there have been worries that sophisticated technology, especially facial recognition software, has been used to spy on and silence critics of the government.[24] Despite being touted as aids for public protection, these devices such as "facial recognition, AI-based monitoring systems, and censorship technologies" are frequently employed to monitor and quell opposition among the populace.[25] Adopting these technologies would give these governments the ability to restrict access to external content, control what their populations see online, and bolster their

[21] Alpermann, Björn, and Malzer, Matthias: "'In Other News': China's International Media Strategy on Xinjiang—CGTN and New China TV on YouTube", *Modern China*, vol. 50, nº 2 (May 2023), pp. 135-178.

[22] Pandey, Kalpana: "Chinese notion of cyber sovereignty: Building an alternate digital order", Observer Research Foundation Expert Speak, April 2023, at https://www.orfonline.org/expert-speak/chinese-notion-of-cyber-sovereignty-building-an-alternate-digital-order

[23] Yang, Xiaofeng, Yang, Qian, & Wilson, Christo: "Penny for Your Thoughts: Searching for the 50 Cent Party on Sina Weibo", *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 9, nº 1 (August 2021), pp. 694-697.

[24] "Uganda: Rights Concerns Over License Plate Tracking Surveillance System Jeopardizes Right to Privacy", *Human Rights Watch,* (August 2019), at https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking#:~:text=(Nairobi)%20%2D%20Uganda's%20new%20surveillance,government%20should%20scrap%20the%20system.

[25] Miracola, Sergio: "How China Uses Artificial Intelligence to Control Society", ISPI, June 2019, at https://www.ispionline.it/en/publication/how-china-uses-artificial-intelligence-control-society-23244..

own narratives. The proliferation of these surveillance tools gives rise to a new kind of digital territoriality in which governments keep an eye on and control their citizens' online behaviour in order to keep foreign ideas out of their virtual borders while any subsequent foreign criticism of such practices that emerges as a response is a further nod towards the establishment of virtual borders within the cyber domain.

Table 1. A list of Chinese policies aimed at solidifying network sovereignty

China's Path to Cyber Sovereignty	Year	Policy Description and Impact
Golden Shield Project	1998	Globalized digital authoritarianism, inspired internet censorship
Great Firewall Project	1998-2009	Contributed to the fragmentation of the open internet
Regulations on the Administration of Internet News Information Services	2005	Tightened state control over online news, restricted foreign influence, authoritarian media regulation globally.
Cyberspace Administration of China (CAC)	2014	Influenced global norms on state-led digital governance and cybersecurity policies.
Global Initiative on Data Security	2020	Promoted state sovereignty in data governance, countered Western-led frameworks
Data Security Law	2021	Reinforced state control over data flows, tightened regulations on cross-border data transfers.
Personal Information Protection Law (PIPL)	2021	Established strict data privacy standards and a benchmark for regulating tech giants. Influenced global privacy frameworks with state oversight.
Regulations on Algorithmic Recommendations	2022	Mandated transparency, user control, and censorship alignment in algorithms

2.3 U.S. Strategy

The U.S. has traditionally been major advocate of upholding the openness and free spirit of the internet as a whole, with various campaigns, initiatives, policies and laws highlighting its efforts in this realm. Some of the most prominent tasks undertaken by the American government in this regard are the Open Internet Order, Title II of Telecom Act, Cloud Act, Digital Connectivity and Cybersecurity Partnership, Freedom Online Coalition (FOC), Internet Engineering Task Force (IETF), Let the Internet Flow etc. However, there have been many strong criticisms against these efforts with the main notion being that the promotion of a free and open internet

is essentially just a covert way of having access to data and information on other countries, both allies and foes combined, and using this access to carry out questionable tasks.

One such example would be the U.S. Central Command (CENTCOM) initiated Operation Earnest Voice (OEV), one of the country's more overt attempts at narrative manipulation. Originally created in response to extremist propaganda in the Middle East, OEV was intended to sway opinions abroad by sending sock puppets, or fictitious online personas, to engage in social media conversations in the target regions. The purpose of these fictitious personas was to dispel anti-American myths and promote support for American policy in Iraq, Afghanistan, and other regions.[26] The intention of OEV was to directly influence the conversations happening in cyberspace to promote U.S.-aligned narratives, such as the benefits of U.S. military interventions or democratic governance. Although aimed at countering terrorism, the manipulation of online discourse in foreign digital spaces introduced a top-down, state-imposed narrative[27]. Such operations, when exposed, quite understandably generate distrust in online platforms. Foreign users, upon learning that they might be interacting with fake personas or manipulated content backed by the U.S. government, might grow wary of international discourse.

This erodes trust in online spaces and, in some cases, leads to greater scepticism of foreign engagement, creating a sense of "us versus them" in online communities. The practice of sock puppetry by a state actor can be perceived as undermining the legitimacy of online public spheres. Even in the context of its geopolitical rivalry with Russia, the U.S. has utilised narrative-building strategies to influence public opinion in the states of the former Soviet Union and Eastern Europe. The United States seeks to counter Russian influence in these areas by promoting narratives about democracy and human rights through NGOs, media, and cyberspace. Occasionally, however, these acts have sparked allegations of American meddling, further dividing the public and inflaming anti-American sentiment in nations that support Russia.

James A. Lewis in a 2019 article has elaborated further that, indeed, the birth and commercialisation of the internet has brought western and American ideas to previously insulated nations. In a domain as elusive and abstract as cyberspace, cultures are bound to interact with each other at some point due to the numerous interconnections that exist even at the remotest of locations. American and western-driven globalisation sought to amalgamate all types of human values together as an embodiment of human progress but was instead met with increasingly widespread discontent. Instead of deeper amalgamation, we see the resurgence of nationalism, as the demand to protect one's own values and cultures are being realised in an explosive manner.

This entire development has been deemed to be quite the opposite of what was initially visualised by the American-led western style of international governance (*Please refer to Table 2 for a list of U.S. efforts to democratise the internet*). The idea that was in the minds of the earliest internet visionaries regarding "one world, no borders" has instead been made to meet its anti-thesis. According to the author, there is a rising trend in which a lot of countries desire to return to an earlier model of global order (pre-1945), where there were lesser constraints, much greater emphasis on sovereignty and minimal external interference. The use of the internet-driven cyberspace to bridge divisions and gaps between various societies and

[26] Fielding Nick and Cobain Ian: "Revealed: US spy operation that manipulates social media", *The Guardian*, 17 March 2011, at https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks,
[27] United States Central Command, Office of the Chief of Staff, 2022, at https://documents2.theblackvault.com/documents/centcom/22-0091.pdf

communities has instead ended up sharpening existing conflicts and leading to new ones, thus making international cooperation far more difficult to achieve.[28]

2.4 European Union Strategy

In an article, Barrinha and Turner affirm the idea that the European Union (EU) is concerned about the internet becoming increasingly 'westless', or less Western-centric. This suggests that, as a global actor, the EU's primary objective in cyberspace is to reject non-Western ideologies and reinforce a Western-centric barrier within the internet. With regards to countries like Russia and China, the authors suggest that there is indeed a very directly observable attempt at territorialising cyberspace by the respective leaderships. Countries like India, South Africa and Brazil follow a more flexible approach with respect to cyber conduct, depending upon the present state of affairs. With cyberspace still being a very fresh and largely uncharted domain, much of the world remains significantly divided on various issues in this field – net neutrality being one of the most widely debated issues pertinent to the matter at hand.[29]

Moreover, the push for a freer and more open cyberspace by the west has resulted in various countries, including western ones, becoming increasingly concerned with lack of regulations that come with it. States see cyberspace as an unconstrained arena for espionage and coercion, and several powerful states also support cybercrime, either as a tool of state power for simple profit. The EU mentioned that it is open to active participation of non-state actors through multistakeholderism (Raymond & DeNardis, 2015). When discussing the scope of cyber-crime at the AHC in 2022, it greatly differed from the stance of Russia and China by discouraging the committee from including broad definitions of the term and instead adding only descriptions of specific activities within the term. This was interpreted in many ways, with some claiming that the EU's stance would then allow other un-defined activities to continue scot-free as they would not fall within the scope of cybercrime.[30]

Figure 2 - US #LetItFlow Campaign for Network Neutrality

Source: Talking Tech, at https://www.usatoday.com/story/tech/talkingtech/2017/12/14/net-neutrality-rules-dead-my-internet-bills-go-up/952839001/

[28] Lewis, James A.: "How the Cyberspace Narrative Shapes Governance and Security", Observer Research Foundation, October 2019, at https://www.orfonline.org/expert-speak/how-the-cyberspace-narrative-shapes-governance-and-security-56874

[29] Barrinha, Andre & Turner, Rebecca: "Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India", *Contemporary Security Policy*, vol. 45, nº 1 (October 2023), pp. 72–109.

[30] Resolutions and Decisions adopted by the General Assembly during its seventy-sixth session. Volume III. 25 December 2021 – 12 September 2022. General Assembly Official Records Seventy-sixth Session Supplement, nº 49.

Table 2 – A list of U.S. efforts to promote a democratic global internet

U.S. Promotion of Open Internet	Year	Policy Description and Impact
Internet Engineering Task Force	1996	Advanced open internet standards, promoted global interoperability, and influenced the development of non-proprietary, inclusive internet protocols worldwide.
Title II of Telecom Act	1934, 2023	Classified broadband as a public utility in the U.S., enabling net neutrality protections
Open Internet Order	2010	Enforced net neutrality principles, prohibiting ISPs from blocking or throttling content
Freedom Online Coalition	2011	Promoted global internet freedom, advocating for human rights online, opposing censorship, and supporting democratic governance of the internet
#KeepItOn	2016	Mobilized global advocacy against internet shutdowns, highlighting their human rights impact and pressuring governments to maintain access to the internet during crises.
Cloud Act	2018	Facilitated cross-border data access for law enforcement, balancing privacy concerns with national security
Digital Connectivity and Cybersecurity Partnership	2018	Promoted secure, open internet infrastructure and digital inclusion, fostering global cooperation on cybersecurity and digital economic growth.
Broadband Equity, Access, and Deployment (BEAD)	2021	Aims to expand high-speed internet access in underserved areas, reducing the digital divide.

3. Deepening Divisions Over Net Neutrality

In the present day, perhaps one of the most widely debated aspects with respect to the internet is also responsible for causing a great deal of divisions amongst countries and their respective policy makers, i.e., the matter of "Net Neutrality", a greatly advocated term by the western hemisphere of the world. The advocacy of Net Neutrality by the US and the EU is often framed as a normative stance that aligns with liberal democratic values of free expression, open markets, and competition. The idea of a worldwide, networked internet that serves as a marketplace for goods and services is the foundation of the US and EU's narrative surrounding net neutrality.[31] This is consistent with their narrative, which holds that gains a liberalised global system should encourage competitiveness, creativity, and free speech. Net Neutrality may eventually be perceived by other states that disagree with it as a clandestine means by

[31] Regulation (EU) 2015/2120 of the European Parliament, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120.

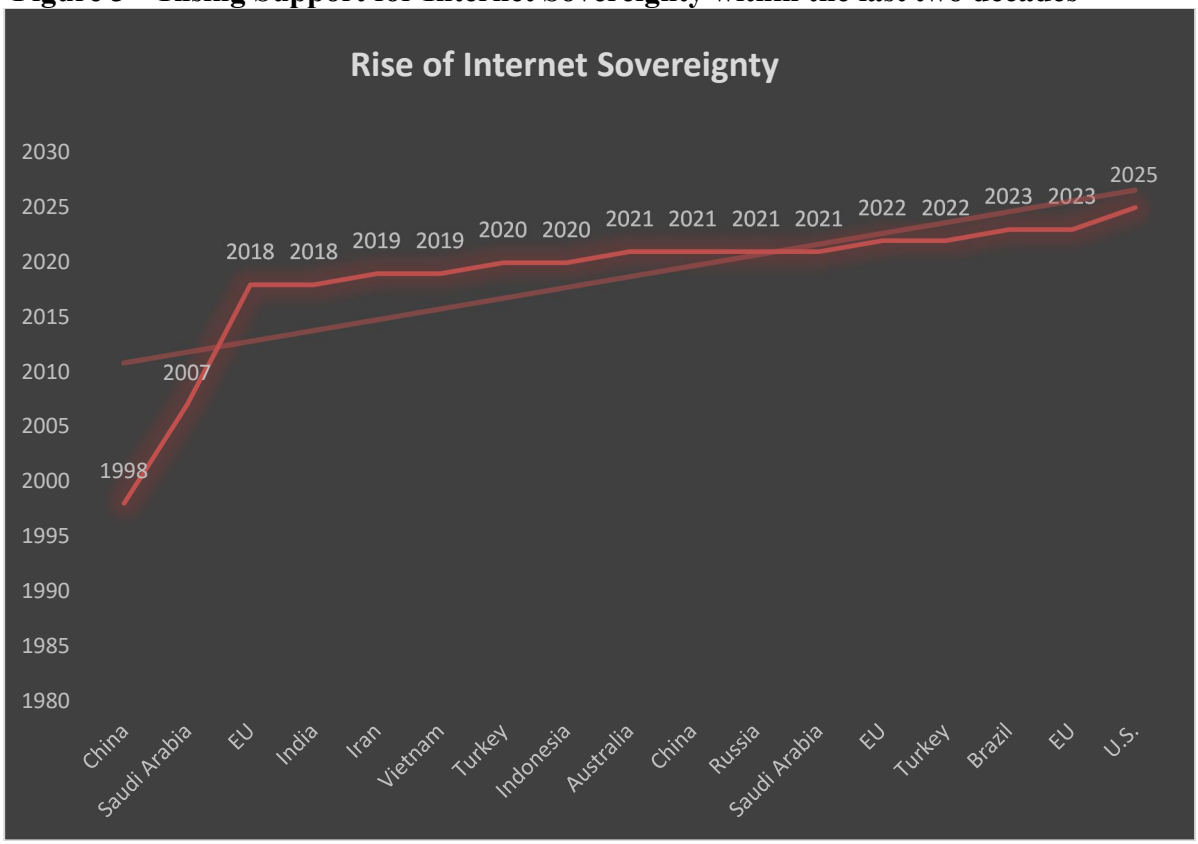
which Western countries continue to control global information flows, exacerbating the already existing imbalance in the international system. According to this perspective, Net Neutrality is an imposition of Western ideas on non-Western states rather than an objective benefit. (Marsden, 2011)[32] The notion of the western powers is at odds with that of the nations that support the narrative of cyber sovereignty advanced by China and Russia. This exacerbates the situation and creates a global cyber regime that is either pro-autocratic or pro-democratic, further fracturing the international community.

In many ways this ideological clash between a free and open internet advocated by the US led west and countries that subscribe to the Russian and Chinese model of internet sovereignty might result in what is known as the "Splinternet" which is a dispersed internet composed of various digital ecosystems representing different geopolitical blocs (Lemley, 2020).[33] Countries such as Saudi Arabia, Turkey, and India may find it more difficult to uphold Net Neutrality in favour of methods of internet governance that conflict with the opposing demands of defending national interests and embracing international norms. Consequently, this gives rise to regional internets customised to the political and economic objectives of particular states or areas. For example, India is demonstrating how nations are negotiating this challenging digital landscape by attempting to find a compromise between the need to control content for social cohesion or national security and an open internet (for example, by outlawing Chinese apps like TikTok in 2020.[34] These acts create a digital economy that is geographically fragmented, which is different from the western push for open internet ideals.
Control over the infrastructure of the internet is another issue brought up by the Net Neutrality controversy. A large portion of the global internet infrastructure is controlled by US and EU businesses, including ISPs and tech behemoths. This leads to an underlying contradiction: despite promoting an open, neutral internet, Western actors continue to hold substantial control over the corporate and physical web layers, resulting in an imbalance of power. Opponents of Net Neutrality may contend that it exposes them to influence from tech companies based in the West. The US and its allies view Huawei's efforts to develop 5G infrastructure globally as a possible security risk, which has resulted in prohibitions in a number of nations. However, China sees the US's attempt to uphold its technological superiority in the Huawei ban. This setback strengthens the belief that the US and EU's system narrative of domination includes global control over internet infrastructure

The two graphical visualisations below are intended to depict the trajectory of both ideologies of Network Sovereignty and Network Neutrality over the years since global access to the internet was provided. In Figure 4, it can be seen that despite the support for democratisation and openness of the internet began a few years earlier than its counterpart, the concentration of the countries advocating in favour of it, show little variety. Whereas, in Figure 3, the countries advocating in favour of network sovereignty seem to display more variety and the number of initiatives taken in favour of network sovereignty are also higher than the ones for net neutrality. The overall trend, showcases a definite rise in both types of efforts, indicating the fortification of two different sets of ideologies regarding the operability of the internet, hence the resultant "Splinternet".

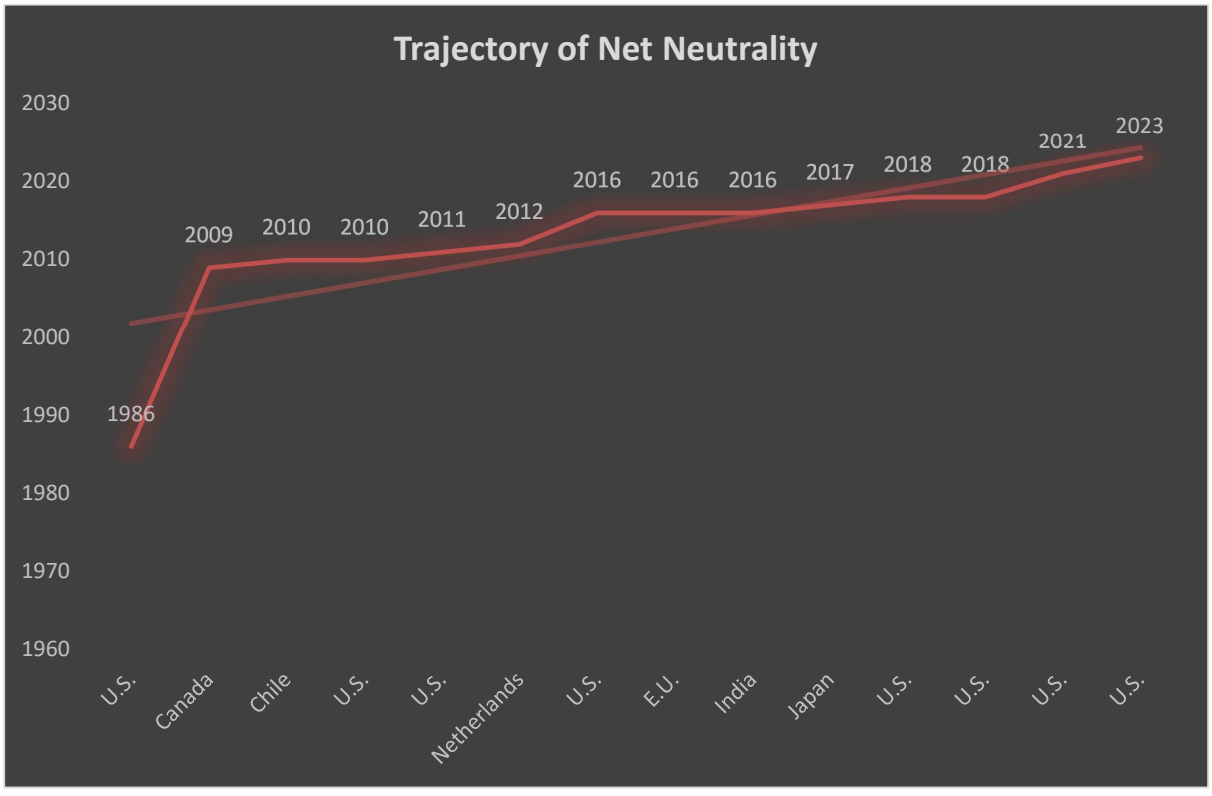
[32] Marsden, Christopher: "Network Neutrality: A Research Guide", in Brown Ian (ed.) (2013) *Research Handbook on Governance of the Internet*, Cheltenham, Edward Elgar Publishing, pp. 419-444.
[33] Lemley, Mark: "The Splinternet", *SSRN Electronic Journal*, nº 555, (August 2020), pp. 1-31.
[34] TRAI: "Recommendations on Net Neutrality", 28 November 2017, at https://www.trai.gov.in/sites/default/files/2024-09/Recommendations_NN_2017_11_28.pdf

Figure 3 – Rising Support for Internet Sovereignty within the last two decades



Souce: Data visualisation processed by the author.

Figure 4. Timeline of network neutrality policies being implemented over the last three decades



Source: Data visualisation processed by the author

4. Virtual Boundaries in the context of Great Power Competition

Barriers often emerge in periods of intense competition between two major powers in the international system due to the inherent need of these powers to assert their distinct worldviews, values, and governing principles. These barriers are not just the result of differences in policy or strategy, but are deeply rooted in contrasting ideologies that frame how each power views itself, the international order, and its role in it. Over time, these ideological differences become entrenched, creating rigid divides that complicate diplomacy, economic interactions, and global governance. In the present scenario, as we traverse through the tides of the fourth Industrial Revolution, similar dynamics may be observed between China and the US, where the ideological differences stem from the two countries' distinct political ideologies—authoritarian state-capitalism in China against liberal democracy in the West. While China sells its model of authoritarian control, state-driven economic growth, and centralised governance as a viable, if not superior, alternative for emerging nations, the US promotes democratic governance, human rights, and open markets.

Major powers frequently engage in a process of "othering" one another as competition heats up, painting the other as morally or ideologically dubious or dangerous (Brons, 2015).[35] This widens the gulf and lends support to assertive measures meant to subdue the opposing force. Ideological othering is also evident in the context of the US-China competition. China presents the West, especially the US, as hypocritical and intrusive, disguising its true goal of upholding global domination behind the rhetoric of democracy and human rights. On the other hand, China is frequently portrayed by the United States and its supporters as an authoritarian nation that aims to destroy democratic institutions throughout the world and impose a surveillance and repression model on everyone else. By reinforcing ideological barriers, this mutual othering makes it more difficult to reach a compromise or comprehend one another.

During these big power struggles, propaganda and information warfare are also frequently seen as means of advancing one's own beliefs while undermining those of one's opponents. As a result, the ideological gap widens as both sides solidify their positions and see the ideologies of their opponents as essentially dangerous. China and the US have engaged in cyber-propaganda as a result of the expansion of social media and the internet. China uses platforms like Weibo, WeChat, and TikTok to inform people about its governance model both domestically and internationally. In parallel, US-based social media companies like Facebook and Twitter have developed into platforms for the propagation of Western notions of free speech and democratic government. The emergence of information echo chambers, which split online environments into fragmented zones where opposing sides' narratives predominate within their respective spheres of influence, further solidifies ideological divides.

5. The Role of Non-State Actors

The establishment of virtual boundaries heavily relies on the involvement of tech titans, particularly Chinese and American companies. Global corporations like Google, Facebook, Apple, and Amazon (in the United States) and Tencent, Alibaba, Baidu, and Huawei (in China) operate on a global basis, but the geopolitical rivalry between the two countries is reflected in their corporate strategies, governance frameworks, and infrastructure reach (Rolf & Schindler, 2023).[36] Content filtering is becoming more common on social media sites like Facebook and Twitter, reflecting the political and legal environments of the U.S. and its allies. As a result of

[35] Brons, Lajos: "Othering, An Analysis", *Transcience, a Journal of Global Studies*. vol. 6, nº 1 (March 2015), pp. 69-90.

[36] Rolf, Steve, & Schindler, Seth: "The US–China rivalry and the emergence of state platform capitalism", *Environment and Planning A: Economy and Space*, vol. 55, nº 5 (January 2023), pp. 1255-1280, at https://doi.org/10.1177/0308518X221146545

these corporations' limitations on content that might go against American principles, an implicit virtual border is created (e.g., hate speech, disinformation, totalitarian propaganda). Through their algorithms and rules, these internet companies effectively create content zones in cyberspace that conform to specific political, cultural, and legal subspaces (Su & Flew, 2020).[37] Many nations and organisations rely on the essential digital infrastructure (cloud services, search engines, social media platforms, e-commerce) provided by U.S. tech giants. This widens the digital divide between countries that use American platforms and those who do not, preferring instead to use Chinese-supplied alternatives.

Chinese tech companies have become important players in the global digital economy. These companies uphold the idea of cyber sovereignty promoted by the Chinese government while operating in a highly controlled and censored atmosphere at home. They have developed into essential tools for the Chinese government in order to further economic objectives, project soft power, and expand China's influence over other countries' digital infrastructure—especially that of Latin America, Africa, and Asia. Chinese digital enterprises are exporting their technologies and governance models to developing countries through programs like the Digital Silk Road, which is a component of the BRI. These nations are frequently drawn to China for financial assistance and embrace Chinese platforms and technologies, bringing their digital ecosystems into compliance with Chinese standards for censorship, data control, and monitoring.

Non-state actors may also include entities such as hacktivist groups, which often take advantage of ongoing rivalries between powerful states to further their own motives which may or may not aligned with the ideological camp of whichever party they choose to side with in said rivalries (Sigholm, 2013).[38] Hacktivists in the US, typically operate independently and are not generally sponsored by the American government (legally at the minimum) and frequently support the principles of democracy. In an effort to draw attention to censorship, monitoring, and China's treatment of political dissidents, American hacktivists have in the past targeted Chinese interests.[39] Operations against China's internet censorship infrastructure have been initiated by groups such as Anonymous, with a common emphasis being the Great Firewall. Attacking websites run by the Chinese government, Anonymous even claimed to be protesting China's human rights repression and censorship in 2011 (BBC News, 2024).[40] They vandalised official websites with statements endorsing liberty of speech and denouncing the Chinese government's autocratic command over the internet. Additionally, American hacktivists often provide assistance to activists from Taiwan, Hong Kong, and Tibet in their quest for greater autonomy or independence from China, thereby strengthening the opposition of these groups to the Chinese Communist Party (CCP).

In contrast, Chinese hacktivists, sometimes known as "Red Hackers," are usually driven by a deep feeling of national pride (U.S. Department of Justice, 2024).[41] While many of these hackers work independently of the Chinese government, their acts frequently serve official objectives. They attack U.S. government agencies, businesses, and media outlets in an effort to promote China's narrative or retaliate against perceived slights against China. One of the most well-known hacktivist collectives is the Honker Union of China (HUC), a group of Chinese

[37] Su, Chunmeizi & Flew, Terry. (2020). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI). Global Media and Communication, vol. 17, nº 1 (December 2020), pp. 67-86.
[38] Sigholm, Johan: "Non-State Actors in Cyberspace Operations", *Journal of Military Studies*, *Sciendo*, vol. 4, nº 1 (November 2016), pp. 1-37.
[39] Lyngaas, Sean: "Chinese hackers targeted U.S. research organizations, officials say", *CNN*, 10 January 2024.
[40] "Chinese websites 'defaced in Anonymous attack'", *BBC News*, 5 April 2012.
[41] "Seven hackers associated with Chinese government charged with computer intrusions targeting perceived adversaries", Office of Public Affairs, U.S. Department of Justice, 8 August 2024

nationalist hackers that was founded in the late 1990s. Their goal was to protect China against what they saw as Western cyberattacks, especially during the height of hostilities over these topics.

6. Conclusion

The rivalry between the U.S. and China has led to the creation of virtual boundaries in cyberspace, which is a paradigm shift that radically alters the character and extent of international relations in the twenty-first century. Ironically, technology and cyberspace have promised to unite people and eliminate boundaries, even as they have created new virtual differences. This phenomenon introduces novel elements of power struggles that stretch beyond geopolitical, technological, and ideological domains, going beyond conventional notions of sovereignty, territoriality, and governance. In addition to being tools of national policy, both countries' strategic use of cyber capabilities and narrative control mechanisms forms the basis for the rebuilding of the world order. The fragmentation of cyberspace into competing spheres of influence reflects the emergence of what scholars characterise as "digital bipolarity", a structural arrangement where the United States and China operate as dual poles of technological and normative authority.[42]

This new bipolarity differs fundamentally from its Cold War predecessor in its pervasive integration of economic, technological, and informational dimensions. Unlike the ideologically driven competition of the twentieth century, contemporary digital rivalry centres on competing models of internet governance: the US-advocated multistakeholder approach emphasizing openness and private sector leadership versus China's state-centric cyber sovereignty model that prioritizes governmental control and national security. Online ideological, political, and economic borders are being formed as nation-states, companies, and non-state entities utilise digital platforms more and more to push their own narratives, manage information, and declare their sovereignty. Due to the divergent conceptions of the internet, controlled vs. free-flowing, between the United States and China, the digital landscape is divided, with nations either adhering to one model, a digital democracy or battling for digital sovereignty. This clash does not just remain within the digital sphere but has substantial implications for international relations as a whole; nations are forced to take sides in a dualistic global system, aligning with U.S.-led open and liberal digital order or China-advocated state-centric, controlled framework. The aftermath of this is the acceleration of the establishment of digital bipolarity, which reflects and dramatically buttresses existing geopolitical rivalries and clashing ideologies.

In a divided digital world, cyberspace has evolved into a battlefield for authority, influence, and territoriality rather than promoting world peace. By controlling the information flow in cyberspace, states and non-state actors are able to create and project narratives that align with their national interests, cultural values, and strategic objectives. Narratives in cyberspace thus become a means by which state power can be proclaimed on both a national and global scale. However, this rivalry over digital governance and narrative dominance contributes to the further fragmentation of the international system as a whole. The world runs the risk of moving towards "digital blocs" with incompatible infrastructures, standards, political beliefs, and ideologies in place of a single global digital common. By undermining the multilateral, rules-based order and substituting it with areas of influence based on ideological and technological differences, such forces alter the current international system.

International cooperation on issues like cybersecurity, data protection, or internet governance becomes harder to achieve, as trust between rival blocs diminishes. Moreover, smaller states are pressured to strategically align with one camp, reducing their autonomy and

[42] Xuetong, Yan: "Bipolar Rivalry in the Early Digital Age ", *The Chinese Journal of International Politics*, vol. 13, nº 3 (June 2020), pp. 313-341.

deepening asymmetries in global power relations. The far-reaching consequences of this digital divide also include a phenomenon that scholars of international relations have termed as "weaponised interdependence" in global cyber-networks.[43] China and the United States have both shown that they can use their network hub positions to further strategic goals, forcing even other major, middle, and smaller nations to negotiate technical ecosystems that are blatantly incompatible with one another. This development forces smaller states into a binary choice between alignment with either the Western-led or Chinese-led digital frameworks. It has the potential of leading to fragmentation of cyberspace where some countries such as India, South Korea, Venezuela, Turkey and various African nations are attempting to create their own ecosystem at a national level.[44]

Elementary principles of international relations theory about the nature of territory, sovereignty, and state authority are called into question by the creation of virtual borders through narrative warfare. Understanding power dynamics in cyberspace, where geography matters in novel and complex ways, is outside the scope of traditional geopolitical analysis, which is based on the control of physical territory and material resources. Even beyond the scope of cyberspace itself, The U.S.-China rivalry has led to the rapid progression of techno-nationalism as a fundamental governing factor in technology policy, linking tech-based capabilities directly to national security, economic prosperity, and geopolitical influence. It has manifested in various forms, including export controls on critical technologies, restrictions on foreign investment in sensitive sectors, supply chain security initiatives, tariff wars and the promotion of domestic technological champions, as observed in recent events across the world.[45] The cyber contestation between the U.S. and China is simultaneously a cause and a symptom of larger changes in geopolitical competitiveness, technological advancement, and clashing spheres of influence.

Bibliography

Alpermann, Björn, and Malzer, Matthias: "'In Other News': China's International Media Strategy on Xinjiang—CGTN and New China TV on YouTube", *Modern China*, vol. 50, nº 2 (May 2023), pp. 135-178, at https://doi.org/10.1177/00977004231169008

Barrinha, Andre & Turner, Rebecca: "Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India", *Contemporary Security Policy*, vol. 45, nº 1 (October 2023), pp. 72–109.

[43] Lehdonvirta, Vili, Wú, Boxi, & Hawkins, Zoe: "Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres", *Review of International Political Economy,* vol 32, nº 5 (December 2023), pp. 1-26.

[44] Mehta, Ananya. "India as a Blueprint for Africa's Digital Public Infrastructure", *ORF Expert Speaks* (August 2025), at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120. Last Accessed: September 3, 2025

[45] Bhkari, Shikha: "Techno-nationalism is reshaping geopolitics, global trade", Policy Circle, 6 August 2025, at https://www.policycircle.org/opinion/techno-nationalism-global-trade/

Barrinha, Andre, & Turner, Rebecca: "Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India", *Contemporary Security Policy*, vol. 45, nº 1 (October 2023), pp. 72–109. https://doi.org/10.1080/13523260.2023.2266906

Bhkari, Shikha: "Techno-nationalism is reshaping geopolitics, global trade", Policy Circle, 6 August 2025, at https://www.policycircle.org/opinion/techno-nationalism-global-trade/.

Brons, Lajos: "Othering, An Analysis", *Transcience, a Journal of Global Studies*, vol. 6, nº 1 (March 2015), pp. 69-90.

Bruns, Alex: "Filter bubble". *Internet Policy Review*, vol. 8, nº 4 (November 2019), at https://doi.org/10.14763/2019.4.1426

"Chinese websites 'defaced in Anonymous attack'", *BBC News*, 5 April 2012.

Dalton, Yasmin: "Has globalisation created a "borderless world" in the post-Cold War era?" June 2019.

Fielding, Nick & Cobain, Ian: "Revealed: US spy operation that manipulates social media", *The Guardian*, 17 March 2011, at https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

Fu, Xiaolan, Avenyo, Elvis, & Ghauri, Pervez: "Digital platforms and development: a survey of the literature". *Innovation and Development*, vol. 11, nº 2–3 (September 2021), pp. 303–321. https://doi.org/10.1080/2157930X.2021.1975361.

Green, Kieran, Sprott, Andrew, Francis, Ed, Lafferty, Brian, Hartley Wise, Henry, Molly, Faerber, Grace, and Miller, Frank: "Censorship practices of the People's Republic of China", Centre for Intelligence Research and Analysis, Exovera, 20 February 2024, pp. 56, at https://www.uscc.gov/sites/default/files/2024-02/Censorship_Practices_of_the_Peoples_Republic_of_China.pdf

He, Laura: "China's New Internet Rule Punishes 'Liking' Posts", *CNN,* 30 November 2022, at https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

Lambach, Daniel: "The Territorialization of Cyberspace". *International Studies Review*, vol. 22, nº 3 (May 2019), pp. 482–506, at https://doi.org/10.1093/isr/viz022.

Lehdonvirta, Vili, Wú, Boxi, & Hawkins, Zo: "Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres", *Review of International Political Economy*, vol 32, nº 5 (December 2023), pp. 1-26, at https://doi.org/10.1080/09692290.2025.2489077

Lemley, Mark: "The Splinternet", *SSRN Electronic Journal*, nº 555, (August 2020), pp. 1-31.

Lewis, James A.: "How the Cyberspace Narrative Shapes Governance and Security", Observer Research Foundation, October 2019, at https://www.orfonline.org/expert-speak/how-the-cyberspace-narrative-shapes-governance-and-security-56874

Liu, Kerry: "China's Wolf Warrior Diplomacy (Narrative): Development, Causes, and Political Effects", *Diplomatica*. vol. 6, nº 1 (April 2024), pp. 71-99.

Liveley, Genevieve: "Stories of cyber security combined report", Research Institute for Sociotechnical Cyber Security, February 2022, pp. 4.

Lyngaas, Sean: "Chinese hackers targeted U.S. research organizations, officials say", *CNN*, 10 January 2024.

Marsden, Christopher: "Network Neutrality: A Research Guide", in Brown Ian (ed.) (2013) *Research Handbook on Governance of the Internet*, Cheltenham, Edward Elgar Publishing, pp. 419-444.

Mehta, Ananya. "India as a Blueprint for Africa's Digital Public Infrastructure", *ORF Expert Speaks* August 2025, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120. Last Accessed: September 3, 2025

Miracola, Sergio: "How China Uses Artificial Intelligence to Control Society", ISPI, June 2019, at https://www.ispionline.it/en/publication/how-china-uses-artificial-intelligence-control-society-23244

Miskimmon, Alister, O'Loughlin, Ben & Roselle, Laura (eds.) (2017): *Forging the World. Strategic Narratives and International Relations*, University of Michigan Press.

Pandey, Kalpana: "Chinese notion of cyber sovereignty: Building an alternate digital order", Observer Research Foundation Expert Speak, April 2023, at https://www.orfonline.org/expert-speak/chinese-notion-of-cyber-sovereignty-building-an-alternate-digital-order

Ramen, Aishwarya: "States' use of non-state actors in Cyberspace", ORF Expert Speak Young Voices, August 2023, at https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace.

Regulation (EU) 2015/2120 of the European Parliament, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015R2120.

Resolutions and Decisions adopted by the General Assembly during its seventy-sixth session. Volume III. 25 December 2021 – 12 September 2022, General Assembly Official Records Seventy-sixth Session Supplement No. 49.

Rolf, Steve, & Schindler, Seth: "The US–China rivalry and the emergence of state platform capitalism", *Environment and Planning A: Economy and Space*, vol. 55, nº 5 (January 2023), pp. 1255-1280. https://doi.org/10.1177/0308518X221146545

"Russia: Growing Internet Isolation, Control, Censorship", Human Rights Watch, 18 June 2020, at https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

"Seven hackers associated with Chinese government charged with computer intrusions targeting perceived adversaries", Office of Public Affairs, U.S. Department of Justice, 8 August 2024

Shaleen Khanal, Hongzhou Zhang, Araz Taeihagh: "Why and how is the power of Big Tech increasing in the policy process? The case of generative AI". *Policy and Society* (March 2024), pp. 1-18, at https://doi.org/10.1093/polsoc/puae012

Shen, Fei: "Great Firewall of China", *Encyclopaedia of Social Media and Politics,* vol. 2 (January 2014), pp. 599-602.

Sigholm, Johan: "Non-State Actors in Cyberspace Operations", *Journal of Military Studies*, *Sciendo*, vol. 4, nº 1 (November 2016), pp. 1-37.

Su, Chunmeizi & Flew, Terry. (2020). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI). *Global Media and Communication*, vol. 17, nº 1 (December 2020), pp. 67-86.

TRAI: "Recommendations on Net Neutrality", 28 November 2017, at https://www.trai.gov.in/sites/default/files/2024-09/Recommendations_NN_2017_11_28.pdf

Uganda: Rights Concerns Over License Plate Tracking Surveillance System Jeopardizes Right to Privacy", Human Rights Watch, August 2019, at https://www.hrw.org/news/2023/11/14/uganda-rights-concerns-over-license-plate-tracking#:~:text=(Nairobi)%20%2D%20Uganda's%20new%20surveillance,government%20should%20scrap%20the%20system

United States Central Command, Office of the Chief of Staff, 2022, at https://documents2.theblackvault.com/documents/centcom/22-0091.pdf

Varshney, Gaurang: "The Dark Horse in the Era of AI: The Nvidia Story", *Economic Times* 21 June 2024, at https://brandequity.economictimes.indiatimes.com/news/digital/the-dark-horse-in-the-era-of-ai-the-nvidia-story/111168499

Xuetong, Yan. "Bipolar Rivalry in the Early Digital Age ", "*The Chinese Journal of International Politics*, vol. 13, nº 3 (June 2020), pp. 313-341.

Yang, Xiaofeng, Yang, Qian, & Wilson, Christo: "Penny for Your Thoughts: Searching for the 50 Cent Party on Sina Weibo", *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 9, nº 1 (August 2021), pp. 694-697.