MERICS
REPORT

FRAGMENTING CYBERSPACE

The future of the internet in China

November 2023

MERICS
Mercator Institute for China Studies

FRAGMENTING CYBERSPACE

The future of the internet in China

Kai von Carnap | Antonia Hmaidi | Rebecca Arcesati | Jeroen Groenewegen-Lau

Contents

Exhibits:

Acknowledgements

Auswärtiges Amt

This report was made possible by the support of the German Federal Foreign Office.

The authors would like to thank participants in online workshops in October and December 2022. Ilker Gündoğan contributed important background research. The majority of the research for this report was concluded in December 2022.

MERICS
Mercator Institute for China Studies

MERICS is a research institute committed to the highest standards of organizational, intellectual and personal integrity and independence. MERICS does not accept funding or rewards of any kind that seek to control the direction, content, or findings of its research and projects. MERICS retains sole editorial control over its ideas and products. All views, positions, and conclusions expressed in our publications should be understood to be solely those of the authors' responsibility.

Executive Summary

CHINA AS A DRIVER OF INTERNET FRAGMENTATION

The internet is at a pivotal moment

The internet as a technology and its future global development is at a pivotal moment. It is uncertain whether it can continue to connect ever-growing amounts of people and devices with minimal friction, or whether it may fragment further into a multitude of separated virtual and analog spaces and technologies. China is a major driver of fragmentation as it is creating de facto barriers in its pursuit of making the internet "secure and controllable".

The geopolitics behind this trend is best illustrated by two declarations. Since it was issued in April 2022, the "Declaration for the Future of the Internet" has been signed by European member states, the United States, and 41 other governments.[1] But not by China, which, through its State Council, published its own vision in November 2022 titled "Jointly Build a Community with a Shared Future in Cyberspace".[2] Whereas the "Declaration of the Future of the Internet" mentions human rights and fundamental freedoms in its opening sentence, China's vision emphasizes security, presenting cyber sovereignty as its first basic principle.

Although the differences are clear, European member states, like most countries in the world, also regulate the internet. As a result, what people experience as the world wide web is in fact already a patchwork of many local networks. The EU can even be seen as a force of fragmentation, creating a regional network through regulations like the GDPR. There are also good reasons for Europe to raise security further, as it is increasingly being targeted by misinformation campaigns, cyberattacks and other challenges. At the same time, China's regulations and barriers to access are more stringent and pervasive than anything European member states and the EU are implementing.

To analyze how ideological differences play out across the different components of the internet, this report zooms in on data flows, web applications, internet protocols and digital hardware, each in its own chapter. Together, these four layers provide a representative cross-section of internet infrastructure. They capture most of the trends and issues, arriving at a range of possible responses for European stakeholders.

The report distinguishes between regional discrepancies and more fundamental fragmentation.[3] Regional discrepancies limit how users experience the internet but are relatively superficial. In this type of fragmentation, the internet is understood as a profoundly interconnected digital public sphere where interventions can be implemented and reversed relatively easily. The first censorship efforts through China's Great Firewall are an example of these regional discrepancies, as blocking the IP address of the New York Times, for instance, can be easily reversed.

A second type of fragmentation involves obstructions to the internet's technological fundamentals. This requires complex adjustments to governance rules, technical standards, or the routing system that obstruct devices from connecting or interoperating. Such fragmentation is much harder to reverse. Throughout the different layers, China has moved beyond regional discrepancies to gradually initiate deeper incompatibilities through a mix of technical, commercial and regulatory factors.[4]

Exhibit 1

The ideal internet

Framework by the Internet Society

Source: Graph based on the Internet Impact Assessment Toolkit by the Internet Society.[5]

Each thematic chapter examines both types of fragmentation and their contributing factors. The underlying analytical framework is inspired by that of the Internet Society, a US advocacy non-profit that promotes the internet's open development. Their framework of normative ideals for the internet (see Exhibit 1) aligns with the EU's strategy, "Fit for the Digital Age",[6] and aims for an internet that is both open, globally connected, secure and trustworthy.

This report outlines how implementing this vision is complicated by the transformation of the "Great Firewall of China" into something that is much more structurally embedded in the way China's internet links up with the rest of the world.

Large parts of China's internet are already inaccessible for anyone without a Chinese ID and phone number. Foreign organizations and firms in China struggle to transfer data to their home organizations because of deliberately vague security regulations. Discussions over shared standards and norms are complicated by profound differences in terminology.

Europe must prepare for a more fundamentally fragmented internet

Relying on its multi-stakeholder model, various European actors should ask their Chinese counterparts for clarity and reciprocity. Dialogue is also needed to jointly prevent deep technological fragmentation, which is still relatively modest today, from extending to more areas and making inter-connectivity physically difficult. At the same time, Europe would be well-advised to de-risk from China and prepare for a more fundamentally fragmented internet.

Endnotes

1 | https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet
2 | https://archive.vn/1iXTf
3 | https://www.intgovforum.org/en/content/igf-2022-pn-internet-fragmentation
4 | https://www.weforum.org/reports/internet-fragmentation-an-overview/
5 | https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/
6 | https://digital-strategy.ec.europa.eu/en/events/high-level-multi-stakeholder-event-future-internet

Chapter 1
China's management of data flows: Towards a state-controlled data island

Kai von Carnap and Rebecca Arcesati

DATA FLOWS

Chapter 1
China's management of data flows: Towards a state-controlled data island

Kai von Carnap and Rebecca Arcesati

KEY FINDINGS

- **China increasingly resembles a data island.** Its data governance regime limits the free flow of information and data across borders in favor of sovereign control. Operators of critical information infrastructure and other data handlers have to thoroughly map out their data flows.
- **China's data localization policies fragment the internet.** They raise costs for service providers and multinational companies relying on global data streams. Under the guise of data security, Beijing is also limiting the ability of foreign users to access resources on the Chinese internet.
- **European policymakers have to pay more attention to the security and strategic dimensions of China risks**. China's new data laws will increase concerns around PRC government surveillance and potential data exfiltration.
- **Recognition of data's strategic importance has fueled dispute between China and the US around digital and telecommunications technologies.** These frictions have already influenced the deployment and use of certain internet technologies, triggering commercial fragmentation between digital ecosystems.
- **Transferring data out of China is difficult, but not impossible.** For now, the regulatory regimes of China and the EU may remain interoperable, but it is unclear whether China's experiment in state-managed data flows could tilt the balance towards excessive fragmentation.

1.1 INTRODUCTION: THE MAKING OF CHINA'S DATA ISLAND

Understanding how China's role in cyberspace might evolve, and how it interacts with the global internet depends upon understanding China's many new laws and regulations around data.[1] This rapidly evolving data governance regime overlaps in part with the party-state's structures for censorship and management of online content, but they are not the same.

Two dynamics involving data are causing a governmental fragmentation of the internet. First, China's data localization requirements increasingly limit the free flow of information and data across borders. The country has not yet turned into a data fortress, but it increasingly resembles an island where the government tightly controls which ships can come and – especially – go.

Second, China's security-centric framework treats data, including personal information, as a strategic national asset. By contrast, the EU looks at privately held and personal data primarily through the lens of privacy.[2] When different jurisdictions follow different philosophies and approaches to data governance, some degree of fragmentation may be inevitable.

1.2 DRIVERS OF FRAGMENTATION: DATA IS THE FUEL OF AN INTERNET SUPERPOWER

The CCP's efforts to "recreate the power structures of national governments in cyberspace"[3] are captured in its data governance regime. Data is therefore treated as a national strategic asset, which has led to data localization requirements that present a form of governmental internet fragmentation.

On the one hand, China's leaders have been intensely preoccupied by data exfiltration risks, noting the activities of whistleblowers like Edward Snowden and the color revolutions. Xi Jinping has referred to digital sovereignty as "another terrain of great power competition after territorial defense, coastal defense, and aerospace defense."[4] Data should therefore be localized to minimize undesirable foreign access. Tellingly, China invoked cyber sovereignty and the legitimate public interest exception to justify restrictions on cross-border data flows in WTO e-commerce negotiations.[5] State access to data must be simultaneously ensured to protect against any threats to state security.

China wants to unlock the value of data

On the other hand, China also wants to unlock the value of data to upgrade the domestic economy to higher-level activities in the global value chain. "If data is the new oil, China is the new OPEC," as Taiwanese venture capitalist Kai-Fu Lee put it in 2018.[6] Lee's analogy captured China's natural advantages in the digital economy (its vast population, deep smartphone penetration, and massive data collection). However, data is not exhaustible; unlike oil it can be used repeatedly, if not indefinitely, by multiple users. This is why the Chinese government rather considers data a "factor of production" and is highly focused on developing a national marketplace for data.[7]

By promoting domestic data circulation, Beijing aims to spur indigenous innovation in digital industries (like AI) and stimulate the digital transformation of the whole economy. Some localization laws are therefore the result of the party-state's desire to minimize unwanted cross-border data transfers that would come at the cost of China's economic interests.[8]

Chinese leaders also believe that a secure and controllable data market is conducive to security and development – with the former taking precedence. Radical fragmentation of data traffic would not be in Beijing's interests because too much of the globalized economy, and China's role in it, depend on free data flows. As of 2019, China and Hong Kong accounted for 23 percent of the world's cross-border data traffic, a 7,500-fold increase on 2001.[9]

Within President Xi Jinping's broader cyber sovereignty agenda, China's data protection framework prioritizes national security and sovereign control of China-origin data.[10] This national security-centric view differs from the EU's, which is mainly concerned with individual privacy. The extent to which Beijing regards geospatial, traffic, and even personal data as national resources became obvious when it halted the debut of ride-hailing company Didi Chuxing on a US stock exchange to prevent foreign access to sensitive information.[11]

China's data island is obscuring more and more information, ranging from academic literature to data about strategic industries, from the outside world.[12]

1.3 RESTRICTIONS OF OUTBOUND DATA TRANSFERS CAUSE HEADACHES FOR FOREIGN COMPANIES

Many sectors in China are faced with data localization rules

Many sectors in China are faced with data localization rules – financial services, mapping and surveying, online publishing, cloud services and healthcare.[13] The Cyber Security Law (CSL) reaches even further by mandating local storage for "personal information" (个人信息) and "important data" (重要数据).[14] The Data Security Law (DSL) and the Personal Information Protection Law (PIPL) further codified local storage requirements for important data, "national core data" (国家核心数据)[15] and personal information.[16] Authorities have only partially fleshed out these requirements, and there is still a lack of clarity around what data is considered sensitive.[17]

By demanding that network operators and data handlers thoroughly inspect the data and the associated transfers, instead of simply passing it on efficiently, China forces them to build additional hosting facilities and even limits the services they can provide in its market.[18] Its new Outbound Data Transfer Security Assessment Measures require many data exporters to conduct a cumbersome self-assessment.[19] Operators of critical information infrastructure and other handlers of sensitive data (e.g., operators of autonomous vehicle fleets) are required to map out data and data flows and make decisions based on their nature and recipients.

The CCP's data governance regime that focuses on national security and protectionist economic interests has led to a series of local storage requirements and complex security assessments of data exports. These obstacles heighten the challenges for European multinationals, which find they need to splinter their data systems in two – a separate one for China– which results in high compliance costs and a less efficient internet.

Companies and investors also face uncertainties around what data remains available for free cross-border flows and how it should be managed.[20] To counter negative spillovers for economic growth and innovation, the State Council announced compliance help for cross-border data flows but only for qualified and designated enterprises in a series of measures published in August 2023.[21]

These measures build on the data-port pilot projects that five provincial governments established in local free trade zones since 2018.[22] Data ports provide physical conduits to facilitate data exchange between China and other regions. Most of them aim to be operational by 2025 and will focus on different issues ranging from facilitating digital trade and attracting various industries to protecting security interests. In the future, it is not inconceivable that cross-border data transfer could be managed through these data ports like ship traffic through harbors.

Ultimately, China's bid to create a state-controlled data island raises questions for the future of the internet as a decentralized routing system.[23] Under a security-centric data regime, the 2023 measures and the data ports focus less on what type of data can be exported but who is allowed to conduct cross-border transfers and where they take place – "data supervision with Chinese characteristics".[24] In a sign that authorities are being receptive to the concerns of multinational corporations, the CAC issued draft regulations in October 2023 which would make outbound transfers a lot easier, at least temporarily.[25]

Exhibit 2

Towards state-managed data flows

Selective Chinese laws and regulations that include data localization requirements

EFFECTIVE SINCE

JUN 2017

中华人民共和国网络安全法
Cybersecurity Law of the People's Republic of China (CSL)

CII operators gathering or producing personal and important data in China shall store it locally and pass a security assessment to export it.[26]

SEP 2021

中华人民共和国数据安全法
Data Security Law of the People's Republic of China (DSL)

The state is to establish data export controls. The category of national core data is introduced and subject to stricter localization requirements.

OCT 2021

汽车数据安全管理若干规定（试行）
Several Provisions on the Administration of Automobile Data Security (Trial)

Handlers of personal information (e.g., of drivers, passengers, pedestrians) or important data (e.g., maps) shall store it in China and need permission to export it.

NOV 2021

中华人民共和国个人信息安全法
Personal Information Protection Law of the People's Republic of China (PIPL)

CII operators and handlers of personal information reaching certain thresholds shall store it in China. Export may be authorized via four mechanisms.

FEB 2022

网络安全审查办法
Cybersecurity Review Measures (revised)

Online platform operators handling the personal information of more than 1 million users and listing on foreign stock exchanges must pass a cybersecurity review.

JUL 2022

数据出境安全评估办法
Outbound Data Transfer Security Assessment Measures

Detail scope, thresholds and modalities of CAC-mandated security assessment for data exports.

JAN 2023

工业和信息化领域数据安全管理办法（试行）
Administrative Measures for Data Security in the Industry and IT Sectors (Trial)

Companies handling important and core data must undergo a security assessment to export it. The Ministry of Industry and Information Technology must approve.

PENDING

网络数据安全管理条例（征求意见稿）
Network Data Security Management Regulations (Draft)

Proposes expansion of cybersecurity review requirement to more scenarios (e.g., mergers of internet platform operators and listings on Hong Kong stock exchange).

Note: *Draft for Comment, November 2021

Source: MERICS summary based on the cited laws and regulations.[27]

1.4 CCP ACCESS TO DATA POSES A DILEMMA FOR THE EU

A fundamental dilemma for data transfers into China is that some countries do not trust Chinese internet and technology companies with their data. Since the CSL came into force, the party-state's ability to compel access to data, including encryption keys, has become a major headache for foreign firms.[28] Apple reportedly handed over encryption keys after it moved Chinese customers' data to state-owned servers, giving government access to sensitive information such as location, photos, and emails.[29]

Beijing asserts jurisdiction over citizens' data rights

The EU's approach rests on the principle that individuals should have control of their data. In contrast, China's party state asserts jurisdiction over citizens' data rights. Localization empowers digital censorship and other forms of digitally enabled repression. In Xinjiang, for example, collection of residents' data – facial data, voiceprints and online activity – is a key tool for repression against Muslim ethnic minorities.[30] Personal information becomes a source of state power, to the detriment of fundamental rights.

The new data laws should intensify the concerns in the EU about Chinese government surveillance and potential data exfiltration, which have already lead to restrictions on telecoms equipment vendors Huawei and ZTE.[31] Putting regime security first, the DSL obligates all PRC citizens and organizations to protect the state.[32] They must share data with the authorities on request or face financial penalties.[33]

State bodies do not need to obtain individuals' consent to harvest their data.[34] The Personal Information Protection Law (PIPL) only constrains mishandling of personal information by commercial actors. When over a billion records were leaked from a Shanghai police database in July 2022, authorities censored internet commentary and summoned executives from database host Alibaba Cloud.[35]

The party state's claims over swaths of individual and commercial data puts European data transfers to China in question. China's political and legal system clearly does not match EU standards of legality, redress, necessity, and proportionality, and has no independent data protection authority.

Moreover, Chinese tech firms that collect personal information from EU citizens cannot guarantee that such information, if sent to the PRC, would not be shared with authorities (see case study). As scholar Lizhi Liu has said, Chinese tech firms must either cultivate deep ties with the party state at home to reduce political risks or prove their independence to overseas regulators to expand globally.[36] Those domestic ties are being increasingly codified in Chinese law.

1.5 THE FUTURE OF DATA FLOWS BETWEEN THE EU AND CHINA

The party-state's push to gain access into both data and its circulation raises questions about the future of European data transfers to China. It can be hard for policymakers to assess what strategic value the party state may extract from data collection activities in the EU, not least because data is a non-excludable good: different entities can derive different insights from the same data set.

The strategic importance of data has also fueled the US-China dispute around digital and telecommunications technologies, with potentially far-reaching consequences for global

networks and commercial digital ecosystems. Worried about potential data exfiltration and Chinese government surveillance, the US government has taken steps that limit connectivity with Chinese networks or restrict PRC-origin digital and ICT technologies.

The announcement of the so-called Clean Network program by the Trump administration in the United States in 2020 has led to a splintering of digital business ecosystems.[37] For instance, US politicians and regulators sought to ban the sale of telecommunications equipment made by Huawei and ZTE.[38] Other frictions concerned undersea cable projects in the Asia-Pacific region. In 2020, US government agencies ordered the Pacific Link Cable Network's Hong Kong connection be dropped, citing "the PRC government's sustained efforts to acquire the sensitive personal data of millions of US persons" and the PRC's intelligence and cybersecurity laws.[39]

European policymakers have paid less attention to the security and strategic dimensions of China-related risks than to data privacy issues. Yet, evidence of Beijing's global data-collection ambitions is plentiful, for instance, China's state-sponsored hacks of the US Office of Personnel Management and of credit reporting agency Equifax.[40] The Biden administration responded by renewing the Commerce Department's powers to assess and counter risks from firms in ICT and tech linked to "foreign adversaries."[41]

Critics have rightly warned against Washington's overreaction, especially given the US lacks federal data protection laws, leaving citizens vulnerable.[42] US government actions and proposals – halting subsea cable projects or calls for a TikTok ban – undoubtedly fragment the internet. However, the EU too should be prepared to deal with data security issues involving PRC technologies. Finding the right balance between security and openness will be hard, but a risk assessment is overdue.

China is building a tiered protection system

Meanwhile, at present, China's data economy is no fortress, and its regulatory regime may even remain interoperable with the EU's. China is building a tiered protection system, where data classes trigger varying degrees of scrutiny based on sensitivity thresholds. Strategic categories, like mapping and genetic data, must stay in the country, but in principle a lot of data can leave upon approval. Getting data out of China is difficult, but not impossible (see Exhibit 3). Importantly, data localization requirements mainly affect larger enterprises.[43]

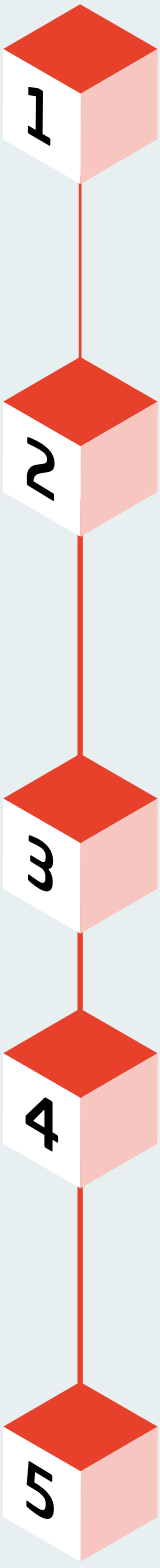
It is unclear whether China's experiment in state-managed data flows, with its vague national security requirements and broad discretionary powers, will preserve interconnection or tilt the balance towards excessive fragmentation. This will depend on how China's data laws are enforced, especially whether regulators go through with the envisaged relaxation of outbound security assessment requirements.

European actors may need to accept some degree of fragmentation induced by China in the data layer. For example, like Apple, foreign automakers BMW and Tesla have opened local storage facilities to comply with China's data laws.[44] The government could compel access to sensitive personal data collected by autonomous vehicles sold in China. This allows a scenario where public security organs can ask BMW to unlock access to in-vehicle conversations for political surveillance.

Exhibit 3

Getting data off the island is difficult, not impossible

Simplified flowchart of China's outbound transfer regime



DO CHINA'S DATA LAWS APPLY? YES IF

- Data processed within China
- Processing overseas but involving important data in China, or data belonging to Chinese individuals for the purpose of providing services or analyzing behavior

AND

- Storage overseas
- Data "provided" to organizations overseas
- Access to data stored in China from abroad
- Access request by foreign judicial and law enforcement bodies (requires permission)

WHO IS AFFECTED?

- Normal data handlers
- Special handlers (e.g., auto data controllers)
- 'Critical information infrastructure' (CII) operators
  - Damage/data leakage could severely harm national security, socioeconomic interests, public interest
  - Operate important network infrastructure and info systems
  - In industries such as telecoms, energy, finance

  OR
  - Business affects critical industries, economic lifeline or govt services (e.g., ride-hailing apps)

WHICH DATA?

- Normal data (incl. certain personal information)
- Personal information
- Sensitive personal information
- Important data
- National core data

WHEN DOES AN OUTBOUND DATA SECURITY ASSESSMENT APPLY?

- CII operators
- Special handlers (in some cases)
- Processors of important data, personal information of 100,000 people, or sensitive personal information of 10,000 people
- Other circumstances at CAC's discretion
- When does a cybersecurity review apply?
  - CII operators
  - Controllers processing personal information of 1 million people and listing abroad
  - Other circumstances at CAC's discretion

ALTERNATIVE MECHANISMS FOR PERSONAL DATA TRANSFER

- EU and China conclude cross-border data transfer pact
- Personal information protection certification
- Standard Contractual Clauses (SCCs)
- Cross-border data transfer pilots in Chinese provinces (e.g., Hainan, Shenzhen)

Source: MERICS

China is intent on shaping the rules of the game. Through its Digital Silk Road initiative, Beijing promotes exports of digital and telecoms infrastructure, technologies, and services, as well as its style of data sovereignty as a contrast to Western data governance.[45] China's Global Data Security Initiative (全球数据安全倡议) – in part, a bid to influence data governance – is endorsed by Russia, Pakistan, the Arab League, and Central Asian states.[46]

However, China's bid to foster its own data coalitions could be restricted by its own policies. Beijing wants to secure preferential data-sharing agreements and raise its profile in global data governance to expand its digital economy and trade. But balancing interoperability and state control may prove untenable. The bold experiment to build a state-controlled data market and cross-border transfer interfaces could undermine the trust of market actors who still favor a free, open, and decentralized internet.

CASE STUDY

CHINESE GENOMICS COMPANY BGI IN EUROPE

The case of China's leading genomics company, the BGI Group, shows the global implications of Beijing considering personal information a national asset. In 2018, the Ministry of Science and Technology fined BGI for illegally exporting certain human genome information.[47] Regulatory developments suggest Beijing regards it as 'important data',[48] and outbound transfers of genetic information such as DNA are prohibited. China-based scientists face growing problems sharing such data with foreign partners, which harms research collaboration.[49] Nonetheless, Beijing exploits domestic genetic data for population control and surveillance, often without the data subjects' consent.[50]

In 2020, the Polish Academy of Sciences canceled a partnership with BGI to create a genomic map of the nation.[51] The academy responded to a warning issued by US national security circles that granting BGI's access to genetic data from foreign populations might allow the Chinese military to identify vulnerabilities.[52] BGI works with the People's Liberation Army on genetic research, both for medical purposes and to "improve population quality."[53]

Endnotes

1 | https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684.
2 | https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
3 | M. Mueller (2017), *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace,* Cambridge: Polity Press.
4 | https://archive.ph/b4zee#selection-429.1449-429.1564.
5 | Joint Statement on Electronic Commerce, Communication from China, INF/ECOM/32, 9 May 2019, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/19.pdf&Open=True. The EU too places privacy protection above the free flow of data in trade agreements. China, however, has tried to carve a wider policy space for itself to impose security-motivated localization. See: https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf; https://archive.is/F3SSV.
6 | https://asiahouse.org/news-and-views/kai-fu-lee-age-ai-china-new-opec/.
7 | He, Alex and Arcesati, Rebecca (2023). "Better Governance to Unleash the Value of Data: China's Practice of Building a Data Trading System". Forthcoming publication with the Center for International Governance Innovation (CIGI).
8 | http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm; https://merics.org/en/short-analysis/china-activates-data-national-interest; https://lillianli.substack.com/p/abridged-data-as-a-factor-of-production.
9 | https://vdata.nikkei.com/en/newsgraphics/splinternet/.
10 | For a discussion of the PRC's vision for cyber sovereignty see, e.g., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421; https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty. On how China's vision threatens a free and open internet, see: https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/. For a legal discussion of the concept of data sovereignty in China, as compared with the EU and the US, see: https://archive.is/F3SSV.
11 | https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002; https://digichina.stanford.edu/work/translation-cac-announces-cybersecurity-review-of-ride-hailing-giant-didi-just-after-its-ipo/; https://digichina.stanford.edu/work/translation-chinese-authorities-announce-2b-fine-in-didi-case-describe-despicable-data-abuses/.
12 | https://archive.ph/yDugC; https://www.wsj.com/articles/china-data-security-law-ships-ports-court-cases-universities-11638803230; https://www.reuters.com/world/china/off-grid-chinese-data-law-adds-global-shipping-disruption-2021-11-17/.
13 | https://www.tandfonline.com/doi/abs/10.1080/17544750.2019.1649289.
14 | CSL, Article 35, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (English language translation, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/). The CSL did not provide a definition of important data. The 2022 Outbound Data Transfer Security Assessment Measures define important data as "data that, once tampered with, destroyed, leaked, illegally obtained, or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc." Outbound Data Transfer Security Assessment Measures, Article 19, https://web.archive.org/web/20220708014822/http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm; English language translation, https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/.
15 | The category of national core data was introduced in the DSL and broadly refers to "data related to national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc." DSL, Article 21, par. 2. This type of data is to be subject to even stricter protection compared to important data.
16 | The PIPL (Article 4) defines personal information as "all kinds of information relating to identified or identifiable natural persons, recorded by electronic or other means, excluding anonymized information." The term "sensitive personal information" is defined (Article 28) as "personal information which, if leaked or illegally used, may easily cause harm to the personal dignity of natural persons, or severely harm personal or property safety, including personal information on biometrics features, special religious beliefs, specially-designated identities, medical health, financial accounts, and whereabouts, as well as any personal information of minors under the age of 14." PIPL, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml; English language translation, https://www.chinalawtranslate.com/en/Personal-Information-Protection-Law/.
17 | Most of these regulations and standards were never finalized, nor implemented, which generated much confusion among Chinese and foreign companies regarding the scope of permissible data exports. See: Security Assessment Measures for the Outbound Transfer of Personal Information and Important Data, http://www.cac.gov.cn/2017-04/11/c_1120785691.htm; Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (unavailable online as of this report's writing); Security Assessment Measures for the Outbound Transfer of Personal Information (English language translation), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/; Draft Data Security Management Measures (English language translation), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/; Information Security Technology – Draft Guidelines for the Identification of Important Data, https://www.tc260.org.cn/file/2022-01-13/bce09e6b-1216-4248-859b-ec3915010f5a.pdf.
18 | https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.
19 | Outbound data Transfer Security Assessment Measures, Article 5. See also Articles 6 and 9.

20| A senior representative of Germany's largest industry association warned about "data decoupling" and mandatory local storage requirements in China affecting data-driven business models, for example in Industry 4.0, https://www.msn.com/de-de/finanzen/top-stories/interview-diversifizierung-ist-kein-kurzfristiger-schwenk-weg-von-china/ar-AA13WYRr.
21| The measures should stimulate foreign investment and restore global confidence in China's economic recovery https://triviumchina.com/2023/08/14/china-gets-serious-about-foreign-investment/
22| https://merics.org/en/comment/beijings-watchful-eye-all-data-flowing-and-out-china
23| https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/China/Policy-Briefing-Cross-BorderDataTransfer.pdf?__blob=publicationFile&v=2; https://www.merics.org/de/kurzanalyse/beijings-watchful-eye-all-data-flowing-and-out-china; https://www.scmp.com/tech/policy/article/3162601/china-plans-its-first-free-data-port-guangzhou-beijing-eyes-total.
24| https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-regulation-with-chinese-characteristics/2539ECBA4499D555BD8206948AD8F4BB, https://www.cnki.com.cn/Article/CJFDTotal-PZGZ202105012.htm
25| https://merics.org/en/data-export-rules-beijings-silence-hamas-attacks-eu-technology-risk-assessment
26| The category of CII operator in China's cybersecurity landscape has caused much confusion among Chinese and foreign companies. The 2021 Critical Information Infrastructure Protection Regulations defined CII as "important network infrastructure, information systems, etc., in important industries and sectors such as telecommunications and information services, energy, transport, water, finance, public services, e-government, national defence, science and technology and industry, etc., as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest. The rules offered some detail on how sectoral and industrial regulators shall designate CII operators within their respective sectors, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm; English language translation, https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.
27| CSL, Article 37; DSL, Articles 21, 24, 25 and 31; Several Provisions on the Administration of Automobile Data Security (for Trial Implementation) (Draft for Comments), Articles 3, 12, 13, 14, 15 and 18, https://archive.is/CLEz7; English language translation, https://digichina.stanford.edu/work/translation-several-provisions-on-the-management-of-automobile-data-security-draft-for-comment/; PIPL, Articles 38 and 40; Cybersecurity Review Measures, Articles 7 and 10; Outbound Data Transfer Security Assessment Measures, in particular Article 4 (for an analysis of the genesis of these rules, see https://digichina.stanford.edu/work/knowns-and-unknowns-about-chinas-new-draft-cross-border-data-rules/); Network Data Security Management Regulations (Draft for Comments), Article 13, http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm; Administrative Measures for Data Security in the Industry and IT Sectors, art. 21, https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_e0f06662e37140808d43d7735e9d9fd3.html
28| https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218.
29| https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.
30| https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinjiangs-muslims; https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass; https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html; https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy; https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions; D. Byler (2021), *In The Camps: China's High Tech Penal Colony,* New York: Columbia Global Reports.
31| https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem. On the obligations for Chinese citizens and organizations to cooperate with state security and intelligence work, and how they may cause data exfiltration risks for countries choosing to procure 5G wireless equipment from PRC-origin vendors, see: https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.
32| https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.
33| DSL, Articles 35 and 48.
34| PIPL Articles 18 and 35; https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/.
35| https://merics.org/en/short-analysis/shanghai-police-database-breach-exposes-lax-data-protection; https://www.bloomberg.com/news/articles/2022-07-14/alibaba-faces-china-inquiry-over-data-theft-wsj-says.
36| https://www.lizhiliu.com/uploads/6/0/9/8/60987819/liu2021_article_theriseofdatapoliticsdigitalch.pdf.
37| https://2017-2021.state.gov/the-clean-network/index.html.
38| https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat; https://www.axios.com/2022/11/01/interview-fcc-commissioner-says-government-should-ban-tiktok.
39| https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-grant-google-and-meta-licenses-undersea-cable.
https://www.freiheit.org/taiwan/geopolitics-reshaping-internet-east-asia.
40| https://www.justice.gov/opa/press-release/file/1246891/download?utm_medium=email&utm_source=govdelivery;
https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html;
https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

41| https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/; https://www.reuters.com/technology/exclusive-us-examining-alibabas-cloud-unit-national-security-risks-sources-2022-01-18/; https://www.newsweek.com/2022/09/16/beijings-plan-control-worlds-data-out-google-google-1740426.html.
42| https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf; https://www.lawfareblog.com/open-data-market-and-risks-national-security; https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html.
43| https://eusmecentre.org.cn/report/cybersecurity-data-and-personal-information-compliance-eu-smes-china.
44| https://www.reuters.com/business/exclusive-china-plans-new-rules-global-automakers-move-store-car-data-locally-2021-05-27/.
45| https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256.
46| Global Data Security Initiative, https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/202010/t20201029_9869292.shtml (English language translation, https://digichina.stanford.edu/work/translation-china-proposes-global-data-security-initiative/); https://web.archive.org/web/20210401014514/https://www.fmprc.gov.cn/web/wjbxw_673019/t1865301.shtmlhttps://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202103/t20210329_9170559.html; https://archive.ph/4JYAj; https://archive.ph/RLqOk; https://archive.ph/zHqIO.
47| https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3430284.
48| For example, the 2019 draft Data Security Management Measures listed genetic data as an example of important data. Data related to the population, presumably including human genetic information, was mentioned in several guidelines for the identification of CII and important data, such as the Guidelines for the Identification of Important Data.
49| https://www.nature.com/articles/d41586-022-01230-z; https://www.pekingnology.com/p/leading-scientist-calls-on-china; 2019 Administrative Measures on Human Genetic Resources, http://www.lawinfochina.com/display.aspx?id=30506&lib=law; 2021 Biosecurity Law, http://www.npc.gov.cn/npc/c30834/202010/bb3bee5122854893a69acf4005a66059.shtml. In 2022, the Ministry of Science and Technology (MOST) proposed an implementing regulation which added important clarity on the security review process (lead by MOST) required for exporting China-origin genetic information, as well as for sharing such information with foreign entities, https://www.most.gov.cn/tztg/202203/t20220322_179904.html.
50| https://citizenlab.ca/2022/09/mass-dna-collection-in-the-tibet-autonomous-region/; https://www.aspi.org.au/report/genomic-surveillance.
51| https://cyfrowa.rp.pl/biotechnologia/art18943801-polskie-geny-nie-trafia-do-chinskiego-laboratorium.
52| https://www.nytimes.com/2021/10/22/us/politics/china-genetic-data-collection.html.
53| https://www.reuters.com/investigates/special-report/health-china-bgi-dna/.

Chapter 2
Turning walled gardens into a fortified courtyard

Kai von Carnap

WEB APPS

Chapter 2
Turning walled gardens into a fortified courtyard

Kai von Carnap

KEY FINDINGS

- **China's regulators have turned powerful walled gardens into a fortified courtyard.** China's authorities have taken some control over super-apps such as WeChat. They have intervened on anti-competitive behavior and sped up new cyber laws.
- **China's authorities are expanding geo-blocking to prevent foreign access.** Evidence suggests that Chinese internet services filter and moderate foreign access based on geographic location. Restricted access to Chinese online resources already impacts researchers and diaspora networks.
- **Identification and registration requirements pose a risk to online privacy.** Current sign-up mechanisms on platforms suggest authorities aim to make domestic and foreign users identifiable online and that many Chinese platforms use phone number registration as an access barrier for certain countries or regions.
- **Mini programs and quick apps indicate a path towards technical fragmentation within China.** Mini programs were first developed on WeChat, but industry competitor Huawei has responded with quick apps, which are only accessible through Huawei exclusive app store. Both introduce new global technical conventions, including new programming languages, proprietary app infrastructures and compatibility requirements for smartphones.

2.1 INTRODUCTION: FLOURISHING WALLED GARDENS

In China, a combination of economic and political factors gave rise to very successful online platforms.[1] They offer an unrivaled wealth of services and functions and are therefore often referred to as "super-apps". China provided targeted policy support for new technologies, and the digital economy faced little regulatory pressure. Symbiotic relations between companies and government departments flourished.[2]

From early on, content control and censorship of information were part of the country's internet policies.[3] US tech companies were either unsuccessful in adapting to China's market or blocked by censors.[4] China leapfrogged internet development stages; mobile phones quickly became a bigger channel than laptops and PCs. In 2021, China reached the threshold of one billion internet users, of whom 99 percent had access via their phones.[5]

The party state's efforts to regulate and address super apps has two diametrically opposite effects on internet fragmentation. On one hand, bricks are taken out of domestic walls be-

tween platforms, making them more accessible and easier to interact with one another, de facto decreasing domestic commercial internet fragmentation. Chinese state ministries and institutions have targeted internet companies' monopolistic practices, content moderation, recommendation algorithms, and other practices.[6] On the other hand, access from abroad is more difficult as exclusionary practices are increasing that keep foreigners out of Chinese platforms.

2.2 TURNING WALLED GARDENS INTO ONE FORTIFIED COURTYARD

Boasting hundreds of millions of users, WeChat, Alipay, and Weibo have become popular apps worldwide. With most US platforms banned in China, they have become irreplaceable communication channels for the Chinese-language diaspora, research networks, and business communities. In addition, online platforms have gained significance as interfaces of political and social discourse and exchange amidst the global pandemic and rising geopolitical tensions.

Chinese internet services filter foreign access based on location

Against that backdrop, we find that new exclusionary rules and practices on these platforms diminish the remaining interfaces between China and targeted foreign regions. First, Chinese internet services filter and moderate foreign access based on geographic location, deploying opaque, location-based discrimination. To sign up for or participate in Chinese internet services from abroad often requires users to give up significant online privacy and anonymity.

Domestically, China's cyber regulators are breaking up tech-monopolies and reinstate open interaction between platforms. By addressing China's apps and programs, who had built powerful "walled gardens," they reverse a trend of fragmentation. The battle between regulators and the private sector is not over as engineers within these companies are devising novel products that could lead to technical fragmentation (see case study on mini programs and quick apps).

Commercial fragmentation within China's internet may decrease, but as China enforces increasingly restrictive rules of participation against foreign users, new digital barriers along national borders are being built. The CCP is turning the walled gardens developed by China's private sector into state-fortified courtyards. This mix of governmental and commercial action could drive technical fragmentation and deeper threats to connectivity.

2.3 DRIVERS OF FRAGMENTATION: TERRITORIALIZING DIGITAL SPACES

The CCP's political goal to transfer and implement legal codes is a central regulatory driver behind platforms fragmentation. China's internet has seen an unprecedented wave of regulation since Xi's second term as CCP general secretary began in 2017.[7] The early campaign addressed market regulations and guided the broad development of China's digital economy. More recently the concept of a "civilized internet" (网络文明) introduced language on control of global narratives on digital spaces. After the August 2022 China Internet Civilization Conference in Tianjin, regulators published the "Declaration on Jointly Building Internet Civilization" (共建网络文明天津宣言);[8] it speaks of purifying internet culture and cultivating online ethics that fit socialist values.[9]

The notion of a civilized internet implies that areas that could affect China's social or political stability are heavily regulated, while authorities give China's internet companies space to innovate and to further indigenous innovation protected from foreign competition without becoming too autonomous or monopolistic.

As a result, the party introduced user identifiability early on as an essential concept to prevent online mobilization against its one-party rule.[10] Real-name registration was also meant to help prevent online fraud, although scams remain a major problem today. It also raises barriers to "undesirable" foreign content or cyber espionage by making it harder for foreigners to access the Chinese internet.

2.4 REGULATIONS WEAKEN CHINA'S DOMESTIC WALLED GARDENS

China's online ecosystem is dominated by a few super-apps that allow users to do nearly anything within their ecosystems. For instance, WeChat started as an instant-messaging app like WhatsApp, but today offers everything from digital payments, ride-hailing, food takeaway, news aggregation, investments and much more. They amplify internet fragmentation by limiting interoperability and interconnectivity with other parts of the internet.

China's online ecosystem is dominated by a few super-apps

Walled gardens are not exclusive to China, but the position of super-apps is. Many such constructs block external links to other apps, so users cannot share information between them except through screenshots.[11] This blocks legitimate third-party use of these resources.[12]

Lastly, platforms were widely reported to use algorithms to reduce the visibility of content from outside their ecosystems. Content is generally not indexed, so search engines like Google or Baidu would not display it.[13] WeChat's own search function resets URLs after a certain period. This nullifies the internet's inclusivity, ease of access and unrestricted reach.[14]

China's authorities have removed some bricks in the walls around platforms, for example, by requiring them to permit external links to competitors. China's State Administration for Market Regulation outlawed locking in vendors under exclusivity practices, and the Cyberspace Administration of China (CAC) forbade algorithms that restrict information from other online service providers.[15]

However, barriers between the platforms and the wider internet have not been entirely removed. External links must now be added to a whitelist, a more sweeping rule than maintaining a blacklist. Barriers like the lack of indexing and limited search functions also remain in place. This helps censors by making information outside a user's tightly curated feed more difficult to find.

2.5 BLOCKING FOREIGN ACCESS TO CHINA'S INTERNET

Towards the global internet, China's regulators have acted rather differently. Foreign access to China's internet is being limited by expanding the Great Firewall and automatically blocking websites, or by restricting the sign-up options on platforms for foreign users.

China's Great Firewall is evolving. Geolocation-based discrimination against users with foreign IP-addresses restricts content and features on Chinese websites.[16] Effectively some

websites are geo-blocked outside China, returning "403 Forbidden" results. Tianyancha.com, China's biggest company database, is one of many websites that declines foreign access, saying: "According to relevant laws and regulations, our website is not available for use outside mainland China."[17]

Technical workarounds like virtual private networks (VPN) can still hide user locations. But new laws and regulation on "dedicated communication lines" and encryption technologies as well as periodical VPN crackdowns since 2018 make them far less trustworthy and reliable.[18]

No systematic study has analyzed the dynamics and patterns of location-based discrimination, nor does China have consistent regulations or guidelines. The likely goal is to prevent espionage and foreign access as the CAC has increased its prevention efforts in September 2021.[19]

One option Chinese policymakers have discussed is two different versions of websites, for domestic and foreign users. Servers for foreign access would be located in data ports, which would allow micro-blog forums like tianya.com a gateway for safe and orderly foreign access to influence Chinese speakers around the world.[20]

Foreign access is also restricted through sign up procedures for apps and services. Chinese apps use far more extensive identification mechanisms. Users commonly get asked for phone numbers, bank credentials, scans of ID, passport or driver's licenses. China is also one of many jurisdictions that links phone numbers to national IDs.

Tests of 18 popular Chinese online platforms (by market share and global availability) reveal that 13 limit the phone registration options as not all countries' phone number formats will fit (for example, Weibo permits 25 country prefixes). Six platforms limit access to users with China's dialing prefix +86 (see Exhibit 4). None of the 18 services allowed registration via email address only.

Some internet services bar all non-Chinese users from registering. Full use of China's digital currency, the e-CNY, and referencing geolocations through Baidu Maps[21] is limited to Chinese nationals or phones with China's +86 prefix. Apps and websites seem to make ad hoc decisions about location-based registration.

Exhibit 4

Limited by dialing code

AVAILABILITY BY AMOUNT OF PHONE PREFIXES	CHINESE ONLINE SERVICES
Only in China (+86)	Douyin , Kuaishou, Aiqicha, Qichacha, Tianyancha, CNKI
In up to 100 countries	JD.com, Weibo
In between 100 to 200 countries	Taobao, WeChat, Zhihu, WeChat Pay, QQ
In more than 200 countries	Bilibili, Xiaohongshu, Alipay, Ctrip, Qunar

Source: MERICS

None of the 18 services allowed registration via email address only. Anonymity is compromised on Chinese platforms as identifying users across platforms by their phone numbers is easy. These barriers to entry are beyond what is considered justified and appropriate identification in some European jurisdictions, including Germany.

Since 2017, demands have become more stringent as 2012 legislation on ID-based real-name verification (实名制登记) for services beyond banking and finance began to be enforced. After 2017, the Cybersecurity Law (CSL) gave the CAC a strong mandate.[22] The law states that internet companies must obtain real user IDs and must not provide services to users who do not comply.[23] Notably, neither the CSL nor subsequent regulations differentiate between foreign and PRC users.

In 2021, CAC rules for 39 different app types made users' phone numbers the minimum registration requirement. In January 2022, CAC further intensified security-review measures under the slogan "obligatory real name registration, but voluntary username" (后台实名、前台自愿'的原则).[24] Today, implementation of real-name identification requirements on Chinese platforms seems to be progressing but has not yet been fully achieved (see Exhibit 5).

2.6 CHINA'S SUPER-APPS ARE CHALLENGING PRIVACY IN EUROPE

Chinese online services present challenges to seamless digital communication and to privacy. Many global platforms are banned in China, hindering digital communication for diaspora communities, researchers worldwide, and businesses. LinkedIn, for example, initially disabled certain features for China-based users to comply with the laws on the ground. Tougher rules led it to end services there in 2021 and, for a brief period, launch a separate China online platform called InCareer.[25]

China's real-name registration requirements threaten users' privacy online. Its user registration law is not fully enforced for international users; they usually only need to give a phone number. This could change if TikTok and other Chinese platforms opt to implement China's ID law more vigorously. If they do so, it may bring them into conflict with European regulations.

China's real-name registration requirements threaten users' privacy

Apart from TikTok, Chinese apps and websites have almost no global foothold. WeChat has very few global users outside the Chinese diaspora. TikTok is a separate case as it was specifically developed for the global market and, for that reason – according to parent company ByteDance – cut off from its Chinese counterpart, Douyin. Quick apps compete with WeChat in China but do not yet offer a compelling alternative to tools offered by Google or Apple's app stores. However, this could change if Huawei's homegrown operating system, Harmony OS, becomes popular in emerging markets.

But Chinese tech giants are becoming increasingly competitive. They have a strong impetus to export their business models as domestic market growth hits its limits, and the Xi era imposes strategic obligations on China's corporate titans. The EU needs to prepare for this growing competition, not only on its own market but particularly in third countries.

Exhibit 5

Fragmentation by registration

Registration requirements on selected apps and websites in China and Europe

✕ Obligatory input items ／ Optional input items

PLATFORMS IN CHINA	PHONE NUMBER	MAIL	ID	BANK ACCOUNT	PHONE NUMBER	MAIL	ID	BANK ACCOUNT	PLATFORMS IN EUROPE
E-COMMERCE									
Taobao	✕				／	／			Amazon
JD.com	✕								
INSTANT MESSENGER									
WeChat*	✕				✕				WhatsApp
QQ	✕				✕				Telegram
SOCIAL MEDIA & VIDEO									
Douyin					／	／			TikTok*
Kuaishou*	✕				／	／			Twitter*
Bilibili*	✕								YouTube*
Xiaohongshu*		✕							Facebook
Weibo*	／	／			／	／			Instagram*
KNOWLEDGE & BUSINESS									
Zhihu	✕					✕			Quora
CNKI*	／	／				✕			Elsevier
Aiqicha	✕					✕			Google Scholar
Tianyancha	Inaccessible outside of China					✕			Crunchbase*
Qichacha	✕					✕			CBInsight
PAYMENT & FINTECH									
Alipay	✕	✕	✕	✕	✕	✕		✕	PayPal
WeChat Pay	✕	✕	✕	✕					
TRAVEL									
Ctrip	✕				／	／			Booking.com*
Qunar	✕				／	／			Kayak*

Note: *Additional options are provided to register via third-party platforms, such as Google, Facebook, or WeChat and Weibo in China.

Source: This table contains a selection of the most widely used Chinese websites with a varying degree of accessibility based on geolocation and is the product of original MERICS research.

CASE STUDY

WECHAT AND OTHERS DRIVE FRAGMENTATION

WeChat is the epitome of the Chinese super-app that can lock users into their ecosystem. However, its new technical features – or 'mini programs' – curb interconnectivity between different parts of the net and drive technical fragmentation.

WeChat started as a WhatsApp-like instant-messaging app in 2011. It quickly grew into a multipurpose "Swiss Army Knife", with everything from banking to ride-hailing and news. Today, the platform is more akin to a new type of infrastructure or supra-operating system[26] that builds one walled garden within another.

WeChat's mini program (小程序) functionality was released in 2017 and gained 350 million daily active users in little more than a year. Mini programs are cloud-loaded apps, they do not need to be installed on a device, especially useful for small tasks but also popular for viral games.[27]

Programmers can develop apps for the mini-program infrastructure but must use WeChat's proprietary scripting language, Weixin Script, and are only accessible through the WeChat interface.[28] WeiXin Script is based on, but not compatible with, JavaScript, a language often used for interactive features on mobile apps and websites. WeChat's custom tools (called WeiXin Markup Language and WeiXin Style Sheets) increase commercial fragmentation as developers cannot easily make a cross-platform app for iOS, Android, and WeChat.

As WeChat's mini programs compete with the app stores of all Chinese smartphone makers, Huawei and all other Chinese smartphone makers banded together to offer a competitive alternative, "quick apps". These are also cloud only but their inner workings differ from mini programs. They use non-proprietary languages like JavaScript, html and css, based on an emerging mini-apps standard.[29]

Nonetheless, Huawei has indicated quick apps use different design standards to most HTML5 apps, web applications for smartphones and handheld devices.[30] Huawei offers automatic conversion tools, but developers must first submit an ID document, adding a major barrier to the deployment of quick apps.

Quick apps can be run on all recent Android devices, so their use of industry-standard programming languages improves common access, but users must install a special app store[31] that does not run on Apple's iOS.[32] The Quick App Alliance says 1.2 billion smartphones, 18-19 percent of the world's total, support quick apps.[33]

Clearly, Apple and Google have done similarly in their ecosystems. Apple, for instance, also has its own open-source programming language, Swift. One interpretation is that competition is driving these companies to fragment the web into ever more walled gardens. But WeChat generates multiple layers of fragmentation. The first wall is a compatible smartphone; then a restrictive registration process (the second wall); and third, features segmented by geolocation.

Endnotes

1 | Platforms can be described as two-sided or multi-sided markets. In addition to or instead of providing an individual service (such as news websites), platforms facilitate economic transactions between two or more groups of actors. While YouTube, for example, brings together the two groups of content creators and viewers, Facebook connects multiple markets, by providing a chat function for users, advertisements space for companies, a marketplace for products and services, and a gaming platform for third party developers. Big Tech companies, in particular from the US, successfully harnessed the crosspollinating effects of different user groups on platforms (also called network effects), giving rise to new digital business models and economic growth drivers such as personalized advertising based on big data analysis and other forms of platform and surveillance capitalism.
See: Srnicek, Nick (2016). Platform Capitalism.Theory Redux; Zuboff , Shoshana (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power
2 | https://www.chinabankingnews.com/2021/10/11/chinas-fintech-sandbox-projects-approach-120-in-number-16-local-governments-launch-trials/
3 | Hillman (2021) The Digital Silk Road: China's Quest to Wire the World and Win the Future
4 | https://www.bloomberg.com/news/articles/2016-08-01/didi-schools-uber-on-doing-business-in-cut-throat-chinese-market, https://hbr.org/2016/08/the-real-reason-uber-is-giving-up-in-china; https://qz.com/1352137/why-internet-users-chose-baidu-over-google-when-it-was-in-china
5 | https://multimedia.scmp.com/infographics/china-internet-2021/#download
6 | https://merics.org/en/short-analysis/tech-regulation-china-brings-sweeping-changes
7 | https://merics.org/en/short-analysis/tech-regulation-china-brings-sweeping-changes
8 | https://english.news.cn/20220828/3980e4588c964d14897703aac8b2f0a2/c.html
9 | https://archive.ph/7bT8d
10 | https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070682
11 | Brussee, Vincent (Forthcoming 2022). Authoritarian Design: How the Digital Architectures on China's Sina Weibo Facilitate Information Control. Asiascape: Digital Asia 9.3: 207-241.
12 | See Enabler: Unrestricted reachability. Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/
13 | https://yiqinfu.github.io/posts/walled-gardens-china/
14 | https://www.internetsociety.org/wp-content/uploads/2021/11/Enablers-of-OGST-EN.pdf
15 | https://www.chinalawtranslate.com/en/algorithms/ art 15
16 | https://citizenlab.ca/2016/11/wechat-china-censorship-one-app-two-systems/, https://citizenlab.ca/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/
17 | https://web.archive.org/web/20221013114152/https://www.tianyancha.com/
18 | https://www.advant-beiten.com/sites/default/files/downloads/Flyer%20China-VPN%20and%20Encryption_BEITEN%20BURKHARDT.pdf; Crackdown https://www.theguardian.com/world/2022/dec/02/china-brings-in-emergency-level-censorship-over-zero-covid-protests
19 | https://www.china-briefing.com/news/china-cybersecurity-law-cac-solicits-opinions-on-amendment/
20 | https://archive.ph/lJ44c
21 | https://medium.com/trabe/how-to-add-baidu-maps-to-your-application-without-learning-chinese-797b095ffcc8
22 | https://archive.ph/0AbK7
23 | Called network operators in the novel legislation https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/; https://www.nortonrosefulbright.com/en-fr/knowledge/publications/d010d379/china-issues-new-regulations-to-tighten-control-on-internet-forums-and-online-comment-threads
24 | https://archive.ph/0AbK7; https://www.scmp.com/tech/policy/article/3117015/beijing-updates-internet-regulation-include-wide-swath-services-fake
25 | https://www.scmp.com/tech/big-tech/article/3159968/linkedin-launches-new-app-china-without-social-feed-after-shutting, https://technode.com/2023/08/10/linkedin-discontinues-incareer-in-china/
26 | https://www.tandfonline.com/doi/full/10.1080/17544750.2019.1572633
27 | https://www.cnet.com/tech/mobile/nike-mcdonalds-endorse-viral-chinese-jumping-game-tiao-yi-tiao-on-tecents-wechat/
28 | https://wechatwiki.com/wechat-resources/wechat-mini-program-epic-tutorial-guide/
29 | https://quick-app-initiative.ow2.io/page/whitepaper/
30 | https://web.archive.org/web/20221031160919/https://developer.huawei.com/consumer/en/doc/development/quickApp-Guides/quickapp-h5-to-quickapp-introduction-0000001150075595
31 | https://www.xda-developers.com/huawei-quick-apps-alternative-google-instant-apps/ ; one of the reasons appears to be that Quick appsQuick appsQuick appsQuick appsQuick appsQuick apps need to store some amount of user data, for which a compatible Quick App Manager is required. https://drscmedia.eu/6564
32 | Ibid.
33 | https://quick-app-initiative.ow2.io/page/whitepaper/#products-whole-lifecycle-support

Chapter 3
China's quest for centralized control and application-specific networks

Antonia Hmaidi and Kai von Carnap

INTERNET
PROTOCOLS

Chapter 3
China's quest for centralized control and application-specific networks

Antonia Hmaidi and Kai von Carnap

KEY FINDINGS

- **China develops and supports protocols for application-specific networks that oppose general purpose protocols underlying the global internet.** Blockchain projects and IPv6-based proposals could create multiple parallel and mutually exclusive networks and hence contribute to internet fragmentation.
- **Centralized state control is a common characteristic of these protocols.** Chinese political and economic actors lead the push to replace and supplement current internet protocols with other, more centralized protocol management that allow greater state control.
- **China tries to influence global standardization bodies towards state-driven internet governance of the protocol layer.** Chinese actors have pushed to move away from the multi-stakeholder approach of internet governance that undergirds the internet's wide accessibility. They have also repeatedly altered the language in international protocol proposals to increase appeal and buy-in while still pursuing application-specific networks and government control.
- **China has opposed global moves to improve online encryption which would help to keep communication and data exchange secure.** China uses flaws in the encryption systems to achieve policy goals, notably selective filtering, for instance of content on websites.

3.1 INTRODUCTION: CHINA CHALLENGES THE INTERNET'S PROTOCOL LAYER

The internet is based on a system of rules which, at the most basic level, decide how hardware and people can connect and communicate. It governs everything from traffic between end users and servers; to the flow of voltage through cables and chips; to privacy online. We refer to this system of rules as the protocol layer.[1] Two global protocol standards essentially unify and constitute today's internet as they enable maximum technical interoperability and global connectivity, known as the Transport Control Protocol (TCP) and Internet Protocol (IP).[2]

Under Xi, the party state has further developed upgrades or changes to these protocols that could lead to long-term technical internet fragmentation. They would impact connectivity and interoperability of the current set-up of TCP and IP which were the result of a decades-long tussle known as the "protocol wars" that involved governments, engineers, and corporates.

Beijing averts global protocol standards that might weaken its control

Domestically, China has developed innovations that allow to circumvent core functions of rules that are unfavorable to its cyber sovereignty regime, such as enclosed private-access blockchain-based networks. Simultaneously, the party state averts global protocol standard developments that might weaken government control, such as advances in web encryption to prevent selective network observations.

Internationally, China's push for more government control on the protocol layer has not been very successful. Generally speaking, emerging economies strive to close digital divides, while advanced economies want to improve protocols to allow more complex transactions for their future digital economies. These differences are reflected in standard-setting fora. Here, China develops and supports various alternative protocols to establish multiple application-specific networks that offer unprecedented oversight and control capacities.

China develops novel protocols in public-private partnerships to replace basic functions of existing essential standards like TCP/IP. These protocols allow data-specific discrimination and maximize government control and oversight (see case study on New IP, IPv6+, and segment routing).

3.2 CHINA WANTS TO MAKE THE INTERNET GOVERNMENT-CENTRIC

China has openly criticized the current multi-stakeholder model of international protocol standard-making in favor of multilateral, i.e., inter-governmental principles. It has become more strategic – and successful – at pushing its initiatives in standard-setting bodies like the International Telecommunications Union (ITU). Its goal of switching from a multi-stakeholder approach to a governmental one risks a less functional, more fragmented internet as governments alone may lack sufficient technical expertise. Industry and civil society need to be represented.

China's push has politicized what was primarily a technical discussion, complicating decision making and impeding implementation of future internet applications and their underlying protocols such as blockchain, metaverse and Web3 infrastructure.

China's leaders first mooted an "independent Chinese internet" in the late 1990s and backed efforts to develop "next generation internet innovation".[3] In 2016, Xi stressed that China needed independent innovation in "core technologies" (核心技术) to become an "Internet Great Power" (网络强国)[4]. In 2017, he said independence in the protocol layer was part of his ambition for an independent internet.

Subsequently, the "IPv6 Special Action Plan" emerged from the Ministry of Industry and Information Technologies (MIIT).[5] It listed tasks to generate breakthroughs on IPv6 key technologies (e.g., a new type of routing, new internet architecture, and a new addressing system). It also sought to coordinate the expansion of Chinese internet standards in international standards development organizations to gain first-mover advantage.

In 2018, Xi portrayed internet self-reliance as a national and cyber security matter, hence the need for technical "breakthroughs". Soon after, he declared blockchain was "an important breakthrough for indigenous innovation of core technologies" to help China become an "Internet Great Power".[6]

Beijing's policy agenda fuels internet fragmentation by developing internet protocols more suited to application-specific networks, such as IPv6+ and private blockchains. The goal is to build new network technology and information infrastructure that is efficient, permits government oversight and control and can be sold as an alternative to Western technology.

Using blockchain technology for control

Beijing perceives blockchain as a technology that could replace the internet in parts of its digital economy, while providing wider control over a given network. Hence, in 2019, Xi laid out an unparalleled national plan to develop blockchain technology and integrate it deeply with the economy – where it can facilitate digital payments, store encrypted personal data, or police investigations, or spread information fast.[7]

Beijing views blockchain as a technology that could partly replace the internet

China's blockchain projects are exclusively permissioned via a series of regulations enacted since 2017 that banned the development of open blockchains without a central authority. These permissioned blockchain projects are in most cases led by consortia of state institutions, ensuring ultimate party-state control. This means global interoperability is low, since most international blockchain projects are open.

These new digital environments can be vertically integrated to tightly couple the internet domain with government control and security. For example, the Trusted Blockchain Initiative (TBI), led by a Chinese state research institution, is developing a broad ecosystem for mobile networks that can be bundled with China's Smart City and CityBrain plans.

Attempting to override the Domain Name System

China has pushed its views on internet governance through a seemingly unremarkable upgrade of a protocol, called the Digital Object Architecture (DOA). The DOA originated at the Corporation for National Research Initiatives (CNRI) in the US in 2013; it has many legitimate use-cases, especially for libraries. The Digital Object Identifiers (DOI) for academic papers are one such example.

China's proposal – which was rejected – challenged the use of the Domain Name System (DNS) and IP for internet addresses. Its preferred DOA-based address system would switch the web's emphasis from transporting data around networks, to refocus on persistent 'information objects'. Both the accessing device and the object would be identified, and each interaction authenticated.

Evading efficient encryption

Most of the world's internet is moving towards improved encryption for better privacy, less vulnerabilities (to networks and users) and more secure transactions. China has not done so, causing a security divide between China and the global internet.

Additional encryption hinders selective filtering, which is central to the Great Firewall, and the state's control over the internet. Around 2016, the global internet moved toward encrypting most web traffic (by transitioning from the HTTP to the HTTPS protocol),[8] Global HTTPS adoption reached about 50 percent in 2019, which is when China's censors started blocking web traffic from abroad if it was run on HTTPS. In 2020, the Encryption Law strengthened the party state's influence over the development of domestic encryption standards.[9]

Chinese HTTPS certificates are issued by the China Internet Network Information Center (CNNIC), most of them are deemed untrustworthy by all major web browsers.[10]

Recent studies show that HTTPS adoption in China is low. Some of the biggest Chinese browsers, such as Tencent's QQ, have collected and transmitted extensive user data with low encryption.[11] China has banned international platforms like the BBC and Wikipedia for encrypting their websites on updated international standards.[12]

Recently, China has started blocking all requests where the server name is encrypted, both incoming and outgoing. This hinders secure access to its internet from the outside, decreasing de-facto interoperability.

3.3 CHALLENGING GLOBAL STANDARD-SETTING PROCESSES

China's state-centered approach challenges the global set-up of internet standards development organizations, within which it built up considerable influence. These include the ITU and the International Electrotechnical Commission.[13] It has been accused of deliberately repurposing language to fit its own strategic aims (see case study)[14], whereas the Internet Society advocates "the process of standardization is open to all interested and informed parties."

China seeks to make standard setting a matter for national governments

Broadly speaking, China consistently seeks to make standard setting a matter for national governments rather than firms or NGOs. It favors empowering the ITU, a UN body, over the IETF, a multi-stakeholder body, in ways that have led to unprecedented politicization. In 2013, China and Russia jointly pushed for the ITU replace US-led ICANN in charge of the Domain Naming System, citing the revelations of former NSA analyst Snowden that the US was prone to internet spying.[15]

3.4 CHINA'S APPROACHES TO RESHAPE THE INTERNET WILL AFFECT EUROPE

Imbalances exist in global internet security standards. Germany mandated its government institutions to upgrade to the more secure TLS 1.3 standard in 2019, and the migration has begun. The US merely asks institutions to draft migration plans by January 2024.[16]

China's internet is likely to become less "trustworthy". By accessing an unsecured website one risks becoming traceable by government bodies and vulnerable to all kinds of cyber-attacks, including spoofing, malware, and spyware. China's internet is also growing less accessible from outside by blocking of encrypted connections.

Government content can be more readily promoted on an internet built on IPv6+. The Great firewall works through technical friction, making it less convenient or harder to access undesirable content, spreading fear to encourage self-censorship and flooding state-sponsored desired content, thereby drowning out non-desired content. IPv6+ could enable both friction and flooding by prioritizing government approved content. Selective censorship, a mainstay of CCP strategy, could be enabled and made easier.

Internet toll models threaten availability of services between EU and China

Internet tolls known as "sender-pays" models violate important internet principles, but Internet Service Providers (ISP) have reasons to favor them. China's protocol suggestions are marked by identifiability, which enables ISPs to identify data types and discriminate between them. ISPs could charge internet users differently depending on the requested service. Developing countries seeking to close the digital divide may see merits in this, as these protocols could allow the government to prioritize limited bandwidth. Western ISPs, even if they are opposed to New IP, have also advocated for sender-pays[17] to cope with big-bandwidth services like Netflix.

Developing countries that lack resources to build up a general-purpose network may care less about undermining net neutrality. Their markets offer opportunities for China's strong PPPs, able to link hardware and protocol adoption (see chapter 4) and may explain China's support of widespread adoption of global IPv6 standards. These are a prerequisite for IPv6+ adoption.

The internet's general-purpose nature and interoperability would be threatened by IPv6+ or similar application-specific networking. Balancing the risks and benefits is a challenge. For specific use-cases, especially the industrial internet, such application-specific networks – as opposed to the end-user internet – could increase efficiency and alleviate security concerns.

Public-private partnerships challenge EU-China cooperation in future protocols

The party state's "strategic public-private nexus"[18] offers Chinese tech firms guaranteed user bases.[19] In a symbiotic relationship, private companies' protocols are supported by state-controlled entities so long as the protocols follow Beijing's policy objectives.

In blockchain infrastructures, Chinese players Blockchain-Based Service Network (BSN, which has secured a network-node in France), StraitsChain and the Trusted Blockchain Initiative, will compete with European alternatives, such as the European Blockchain Service Infrastructure (EBSI).[20] This would lead to parallel infrastructures because Chinese blockchains cannot inter-operate with international permission-less blockchains.

Global governance is being altered

In internet governance, Chinese actors are becoming skillful at packaging their proposals to appeal to Western audiences, while "repurposing" technical standards lingo.[21] Understanding what China's government leaders mean when using general-purpose technical language is getting harder. China's negotiators have, for example, introduced the notion of a "flattened network" to reduce carbon emissions, a veiled reference to using IPv6+ that can only be understood if Chinese protocol suggestions and their technical effects are well-known.[22]

Chinese actors are skillful at packaging their proposals for Western audiences

CASE STUDY

HOW CHINA PUSHED NEW IP, IPV6+ AND SEGMENT ROUTING INTERNATIONALLY

An essential protocol – the "IP" address system – is transitioning from IPv4 to an upgraded version (IPv6) due to the world running out of IPv4 addresses. However, it has taken the global internet about 20 years to get half-way through global adoption, with huge regional discrepancies.[23]

Since the launch in 2017 of a protocol initiative by the Ministry of Industry and Information Technology (MIIT), China has tried to promote three considerable protocol updates that imply fundamental technical fragmentation. All three protocols emerged from a MIIT-sponsored public-private partnership (PPP) between Huawei, CAICT, and other state actors (see Exhibit 6).

The protocols – New IP, IPv6+, and SRv6 (or Segment Routing via iPv6) – move control of the internet into higher hierarchies and discriminate traffic based on applications. Not only do they allow selective filtering and thus more effective censorship, they also provide the technical basis for content delivery discrimination through highly controversial sender-pays models.[24] Therefore, they go against the Internet Society's principles of decentralized management and a technology-neutral, general-purpose network.

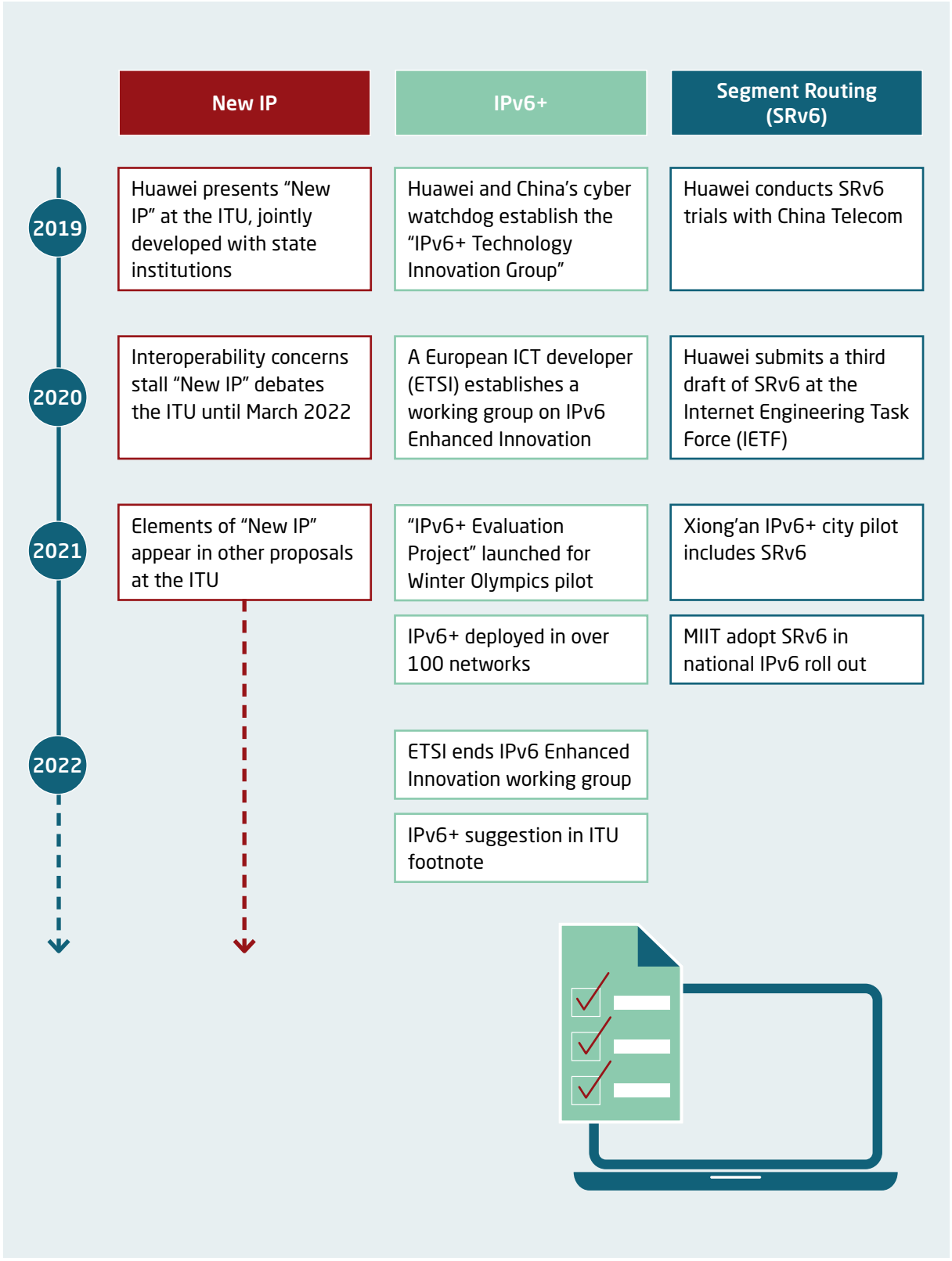
Although these protocols were met with resistance in international standardization bodies, the Chinese PPP lobbied intensely to gather wider global support from developing countries and within the ITU. They continuously seek to change internet protocols over the long term to develop towards global adoption. At the helm of the IPv6+ push, for example, sits the "IPv6+ Innovation Promotion Group", consisting of China Telecom, China Mobile, China Unicom, Huawei, and others. This group was set up under the guidance of the Cyberspace Administration of China (CAC) in 2019. It plans to develop IPv6+ in three phases between 2020 – 2025; the build and integrate phase begins in 2023.[25]

Other countries, especially in the Global South, like South Africa, have already started to adopt IPv6+ in their internet.[26] However, IPv6+ is still experimental and unlikely to become dominant. Similar ideas are being developed in the West for special-purpose networks like the industrial internet.

Exhibit 6

Three paths to change internet protocols

Selected events on the way to establish New IP, IPv6+ and SRv6



Source: MERICS

Endnotes

1 | TCP: transport and transmission of data, IP: address system for devices
TLS HTTPS: security of communication
CDN: content delivery
DNS: web domains
Ethernet: connecting networks through wires
BGP: pathfinder for connecting networks
DNS: index of websites
Blockchain (as an infrastructure): decentralized governance
2 | TCP stands for Transmission Control Protocol and IP stands for Internet Protocol
3 | Austin, G. (2014). Cyber policy in China. John Wiley & Sons; https://archive.ph/wip/NyZq1
4 | https://archive.ph/8t2Av
5 | https://archive.ph/vIkiv
6 | 核心技术自主创新的重要突破口 https://merics.org/en/short-analysis/china-sets-hopes-blockchain-close-cyber-security-gaps; https://archive.ph/3gDcP
7 | https://www.iss.europa.eu/content/chinas-blockchain-and-cryptocurrency-ambitions
8 | https://www.eff.org/encrypt-the-web
9 | https://thediplomat.com/2019/10/decoding-chinas-cryptography-law/
10 | https://archive.ph/ELiFe
11 | https://en.pingwest.com/user/7173440/article, http://www.wsj.com/articles/chinas-top-web-browsers-leave-user-data-vulnerable-group-says-1459198802, https://citizenlab.ca/2016/03/privacy-security-issues-qq-browser/
12 | https://www.bbc.com/news/technology-45098190, https://slate.com/technology/2019/05/wikipedia-china-block-censorship-tiananmen-square.html
13 | https://shop.freiheit.org/#!/Publikation/1334
14 | https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1805482
15 | https://onlinelibrary.wiley.com/doi/10.1002/poi3.296; https://leidenasiacentre.nl/wp-content/uploads/2022/04/Chinas-standardisation-system.pdf
16 | https://csrc.nist.gov/News/2019/nist-publishes-sp-800-52-revision-2
17 | https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/
18 | https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2978880
19 | https://www.coindesk.com/policy/2020/04/24/chinas-national-blockchain-will-change-the-world/
20 | https://www.bsnbase.com/p/main/serviceNetworkDesc?type=RunningCondition, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home
21 | https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1805482
22 | https://twitter.com/kkomaitis/status/1573258603951435778
23 | https://labs.ripe.net/author/stephen_strowes/IPv6-adoption-in-2021/
24 | https://thediplomat.com/2022/08/south-koreas-sender-pays-policy-is-a-threat-to-the-internet/
25 | https://archive.ph/5wDyr; https://archive.ph/EWmmO
26 | https://www.cajnewsafrica.com/2022/11/07/africa-must-speed-migration-to-latest-ip-version/, https://www.telecomlead.com/telecom-equipment/mtn-srv6-based-bearer-network-accelerates-digital-transformation-in-sa-104552

Chapter 4
The disintegration of global supply chains threatens the unity of digital infrastructure

Antonia Hmaidi and Jeroen Groenewegen-Lau

DIGITAL
HARDWARE

Chapter 4
The disintegration of global supply chains threatens the unity of digital infrastructure

Antonia Hmaidi and Jeroen Groenewegen-Lau

KEY FINDINGS

- **Regulatory and commercial fragmentation is growing in the hardware layer of the internet.** China favors domestic vendors and excludes foreign vendors in its quest for greater connectivity. This may eventually lead to more profound technical fragmentation. So far, the commercial benefits of common technical standards outweigh the forces of divergence.

- **China's effort to lessen foreign reliance in digital hardware is driven by a perceived security risk.** China started to systematically build a cybersecurity framework in 2013. Among others, the revelations of former NSA analyst Edward Snowden also contributed to national security considerations overriding economic arguments. The cybersecurity framework has narrowed the space for foreign digital hardware vendors in China's market.

- **China's export success in digital hardware expands its commercial and regulatory fragmentation to the global stage.** It is possible China will disengage, and the global internet will become more divided. Chinese overseas digital infrastructure projects are backed by bilateral agreements, Chinese financing, training and other long-term dependencies. This creates path dependencies that could develop into dividing lines if decoupling between China and the West deepens.

- **Beijing approaches internet infrastructure as a strategic and political asset.** National champions like Huawei and HMN, a provider of submarine cables, get extensive support. Private firms often engage in public-private partnerships. This favors large, vertically integrated firms.

- **Technical fragmentation is on the horizon.** China is willing to use its market power to roll out alternatives to international hardware solutions that are not fully compatible, as seen in the Beidou satellite navigation system and domestic mobile internet standards (3G, 4G and 5G).

- **China is preparing its digital infrastructure for more geopolitically uncertain and less trusting times, and so should Europe.** Chinese commentators urge China to set its own standards if strong global market share fails to translate into standard-setting power.

4.1 INTRODUCTION: GLOBAL COMPETITION OVER THE NUTS AND BOLTS OF THE INTERNET

Hardware provides the internet's basic infrastructure – mobile base stations, cell towers, subsea cables and routers. In recent years, regulatory and commercial fragmentation in the hardware layer has been intensifying. Satellite navigation and user-facing hardware are subject to similar fragmentation trends, especially the semiconductor chips as a field where China and the US are building distinct ecosystems. Over the last 20 years, most countries have sought more control over digital infrastructure in their territory and elsewhere, seeing threats to cyber sovereignty as a challenge for political systems.

However, there are strong commercial arguments for hardware manufacturers to maintain compatibility and interoperability. So far, regulatory and commercial fragmentation has not led to technical fragmentation. Limited interoperability would regionalize markets, destroying earnings and economies of scale.

Fragmentation of the internet's physical infrastructure and technical hardware standards seems unlikely in the short term.[1] But if it happened, the effects would be profound.[2] Chinese base stations in the 2010s used different frequencies for 3G/4G bands; international phones did not always work in China, nor did Chinese ones internationally.[3] Technical fragmentation beyond end-user devices into core infrastructure would signal a fundamental shift.

In 2021, Huawei was the world's largest telecommunications equipment supplier by revenue, with a global market share of 28.7 percent and annual growth of 7 percent.[4] Concerns over the security of Huawei's equipment and Chinese laws led the US to ban Huawei from building its 5G network. Several European countries did likewise. Huawei is still a big player in the Global South, but its business in developed countries has fallen.[5]

China is stepping up efforts to become self-reliant in digital hardware

Meanwhile, China is stepping up efforts to become self-reliant in digital hardware and to boost exports of its hardware products. It is applying its usual mix of domestic protectionism and state support, visible in mobile internet infrastructure (5G base stations), satellite navigation (Beidou), submarine cables, and, increasingly, the satellite internet.

China's efforts to secure its supply chain and Western responses could trigger the commercial and regulatory fragmentation of hardware applications and then drive real technological fragmentation, with different hardware standards evolving in different world regions.

4.2 HOW CHINA IS FRAGMENTING INTERNET INFRASTRUCTURE

China is fragmenting the internet on the hardware layer by protecting its huge domestic market. Its champions in the digital hardware space have increasingly moved abroad. They have leveraged their home market advantages in doing so. Chinese private and state actors now collaborate very closely in trying to influence global standard setting in the hardware sector.

Beijing wants secure and controllable digital hardware. National security concerns are the main driver of the Chinese government's efforts to reduce reliance on foreign digital hardware.[6] At the inaugural meeting of the Cyberspace Affairs Leading Group (now Commission) in 2014, Xi famously said that there was "no national security without cybersecurity, and no modernization without informatization." The leading group's follow through – new

laws, regulations and major entities – to make the Chinese internet "secure and controllable," is increasingly limiting opportunities for foreign digital hardware suppliers.

Cyber security vulnerabilities also play an important role in Beijing's threat perception. If China's network is largely self-sufficient, the thinking goes, attacks that work internationally cannot readily be used there, lessening the risks. This rationale goes beyond network equipment to access hardware, such as phones and computers, and software like operating systems.

Only three state-owned telecommunications companies, China Unicom, China Mobile and China Telecom, are authorized to offer network services – and they favor Chinese suppliers. In 2022, all government entities, including state-owned enterprises, were ordered to use domestic vendors for all their PC equipment.[7] These trends do not impact networking and interconnectivity *per se*, but they lay the ground for an eventual tech transition in which Chinese entities control all relevant equipment.

4.3 BUILDING A CHINESE NETWORK

Industrial policy in China systematically favors domestic players

Industrial policy in China systematically favors domestic players. After the Snowden revelations in 2013, import replacement intensified in the ICT sector, as Beijing put foreign hardware under suspicion of being a potential extension of foreign surveillance and espionage. This is evident in security reviews required of "critical information infrastructure" (CII) providers under China's "multi-level protection scheme" (MLPS).[8] Foreign firms struggle with the lack of clarity with which both categories are defined.

More generally, the Cybersecurity Law, technical standards and a plethora of other regulatory measures collectively discriminate against foreign technology on national security grounds. State-owned enterprises and government bodies have even started replacing all foreign hardware like printers.[9] As a result, China has set off a self-reinforcing cycle where the fact that foreign suppliers are banned from parts of the network reduces the need to work out compatibility issues, which makes it harder for foreign suppliers to remain engaged more generally.

Mobile-internet standards on 3G/4G showed how this plays out in practice. Beijing initially licensed China Mobile to launch 4G TD-LTE, a domestic standard incompatible with the FDD-LTE standard used outside China.[10] It was developed with support from an official sci-tech project on "next-generation mobile internet". China Mobile seized the chance to gain domestic market share. In the megaproject, China Mobile had previously developed its own 3G-technology called TD-SCDMA, which was incompatible with the iPhone, but had low take-up. Beijing took a more strategic approach with 4G. To incentivize telcos to deploy at least a dual system, it licensed TD-LTE before granting FDD-LTE licenses.[11] As a result, domestic equipment makers prioritized TD-LTE, while FDD-LTE was the standard in the rest of the world. As a result, some Chinese phones could not support international frequencies and vice versa.[12]

Across China's networks, the government and state-owned enterprises have favored domestic vendors for political and protectionist reasons.[13] China Mobile awarded some 4G contracts to Alcatel-Lucent, Ericsson and Nokia, but Chinese suppliers got 70 percent of contracts.[14] China has not officially banned Nokia and Ericsson from its 5G network, but by August 2021 their combined a share of China's 5G base-station market was 8 percent. Huawei and ZTE together had 89 percent.[15]

Public procurement data, compiled for this report, shows rising discrimination against foreign suppliers.[16] Government agency tenders for specialized intelligent networks (e.g., in transportation) and government cloud projects tend to go to Chinese telcos. Public-private partnerships (PPP) are key to these projects, which typically go beyond hardware.[17] China's national cloud, a project administered by the State-owned Assets Supervision and Administration Commission (SASAC), will be a self-contained ecosystem providing cloud-computing resources to state enterprises. China Telecom's subsidiary Tianyi Cloud Technology serves the state-owned cloud service market.

China Mobile's tender to upgrade its mobile-cloud architecture specified that applicants must be registered in China. Consortia were not allowed. Unsurprisingly, national champions such as Huawei Cloud and Alibaba Cloud won this and subsequent tenders.[18] Foreign cloud providers cannot access the Chinese market without a Chinese partner.[19]

Promises of equal treatment in government procurement made in August 2023 are unlikely to change this substantially.[20] China has built a fortress made of hardware. With a hierarchical approach to the network, Beijing can monitor 90 percent of China's traffic using only two top-level networks with direct government oversight.[21] Thus, commercial and regulatory fragmentation can lead to technical fragmentation, as management is easier for Beijing at each step.

4.4 CHINA'S HARDWARE EXPORTS CHALLENGE THE UNITY OF THE INTERNET

The successful export of Chinese digital hardware could bring the fragmentation described above to a global stage. This raises the specter of a splintered global internet, divided in blocks. China's provision of a large share of digital hardware worldwide supports its claim to set global norms and standards, making its digital hardware export drive a catalyst of internet fragmentation.

Export promotions play a role: Huawei is a major beneficiary of export credits.[22] However, the Digital Silk Road (DSR) more generally promotes "internet sovereignty" by making Chinese digital infrastructure available elsewhere, helped by soft loans and government training courses. Officials in destination countries learn to control the internet as China does.[23] It can be no accident that Huawei often bundles its networking equipment with surveillance solutions.

Chinese equipment makers are most active in the Global South

Chinese equipment makers are most active in the Global South (see below), though Chinese equipment is also used in Europe. Telekom Serbia, for example, awarded Huawei a EUR 150 million project in 2016 to build high-speed broadband internet.[24] In Germany, Huawei was originally set to play an important role in 5G. Vodafone and Deutsche Telekom are still using some Huawei equipment on cell towers and in core networks, and are sticking with this so far.

However, a recent German law, implementing the NIS-2 directive from the EU, allows exclusion of non-trustworthy vendors. Chinese equipment providers may fall into this category as China's 2017 National Intelligence Law compels equipment and data sharing with its intelligence agencies.[25] An investigation in 2023 led to a compromise that would greatly restrict Chinese vendors' market share in China, although at the time of this writing, no official confirmation for the final rules has been given.

In cloud services, China and the EU's GAIA-X project share a common structural approach, since both treat the cloud as vital public infrastructure provided by PPPs.[26] In the US, private sector firms dominate. Depending on which stance prevails, this might create compatibility issues with internet hardware. If clouds are seen as a public good, they are likely to be organized along national boundaries, with the potential for different standards in each nation.

Generally, Chinese vendors are still trailing US ones in international backbone networks.[27] But in Africa, Chinese companies are building general-purpose and intra-governmental networks and have provided 70 percent of the continent's 4G networks.[28]

Exhibit 7

Selected countries with Chinese hardware in their internet stack

COUNTRY	YEAR	CHINESE COMPANY	TYPE OF SERVICES	STATUS
Argentina, Brazil, Chile, Mexico, Peru	2022	Huawei	Cloud services and data centers	Active
Cambodia	2019	Huawei	5G	Active
Cyprus	2022	Huawei	5G Core Network and RAN infrastructure	Active
Serbia	2016/2022	Huawei	High-speed broadband internet (5G), cameras for facial recognition	Active
South Africa	2022	Huawei	5G network	Active
Thailand	2022	Huawei	5G service in hospital	Active
UAE	2022	Huawei	Specific network for aviation industry, cloud services and data centers	Active
Uzbekistan	2022	Huawei, ZTE	3G, 4G, 5G base stations	In development

Source: MERICS[29]

While US attention has focused on 5G network providers, cloud and data centers may be more important for data security and other types of security.[30] Cloud providers are able to see the data, and usually can transfer data to other clouds in their network without oversight. As soon as data is stored on a cloud in China, Chinese laws apply, and operators can be required to hand over data to China's government. Alibaba Cloud is a partner of the Olympics in Paris.[31] In the Middle East, Huawei provides cloud solutions and business-specific 5G networks.[32]

Chinese companies are exporting China's commercial and business model fragmentation tendencies abroad, while benefiting from support in their home market. China's global reach could drive regulatory fragmentation in the EU and US, despite recent protective legislation.

4.5 CONFLICTS OVER STANDARDS ARE LOOMING

Engaging with China in global hardware standard setting is increasingly challenging. Faced with setbacks, Chinese commentators argue Beijing should simply set its own standards. There is a relatively small risk of immediate fragmentation, but interactions are getting more fractious.

China's international standard-setting drive is increasingly coordinated. It centers on Huawei, a leader in 5G technology, and aims to increase the company's share of standardization patents.[33] When Huawei's 5G-eMBB standard narrowly lost to Qualcomm at the 2016 International Communication Conference, Lenovo had to publicly apologize after voting for Qualcomm.[34]

In contrast, European and US firms often work against each other in setting international standards. This can lead to better technical outcomes but leaves these firms at a competitive disadvantage vis-à-vis China.

As of today, China has contributed more to 5G standardization than any other country, but Sweden, Finland, and the US combined have done more. China has 33 percent of patents declared as standard-essential, followed by South Korea with 27.1 percent. The EU has 17.1 percent of patents, but EU and US patents are cited more frequently and matter more overall to 5G.[35]

4.6 CHINA'S ASSERTIVE DIGITAL HARDWARE STRATEGY HAS TAKEN EUROPE OF GUARD

Europe has responded inconsistently to commercial fragmentation

European governments and firms have responded inconsistently to the reality of commercial fragmentation in the internet stack. Who controls the hardware, controls data and security: China and the US are formulating strategic programs to increase their control over digital hardware – and the data and information flows they enable. Their national security and geopolitical competition in this field will have major long-term ramifications for Europe.

Spying is a concern. The US has been found spying on citizens data, the topic of Snowden's allegations. There have been credible allegations of Chinese spying at the African Union, using Huawei network equipment and Huawei surveillance cameras. China's hardware exports often bundle networking equipment and surveillance technologies.[36]

Submarine cables are also a concern, their exact locations typically kept secret to prevent sabotage or intelligence gathering. European security agencies identify China among countries this critical infrastructure should be protected from – impossible if firms like HMN build and operate them.

EU member states compete with each other for influence in Europe, North Africa, the Middle East and beyond. This undermines any common strategy and allows more coordinated Chinese actors to win digital infrastructure contracts even in Europe.[37]

Even though European firms find themselves in a difficult position, their usual response is to insist on competition and reject government involvement. European telcos have long opted for cheaper Chinese offerings where feasible, as shown by French company Orange's extensive use of Huawei components in Africa. In China, Nokia and Ericsson are both still major players, but they are increasingly being replaced by domestic competitors.[38]

Conflicts will come to a head in key areas like patents used for hardware standard setting. A WTO case is underway against China for blocking European companies from enforcing their rights to key technologies like 3G, 4G and 5G in China.[39] Control over standards and their underlying patents would give Chinese firms a substantial economic advantage.

Europe and Germany find themselves in two conflicting digital dependencies – on China for hardware and on the US for software and applications.[40]

Huawei has been kept out of the core network of German telcos, but it remains a major supplier of Germany's cell-tower equipment, and active in Central and Eastern Europe, especially in cloud, data center and higher-education networks.

The EU has yet to put enough funds or political will into Global Gateway, a project to counter the BRI, to strengthen connectivity within and beyond the EU. Created in September 2021, the digital component has a meager annual budget of EUR 130 million. Moreover, its value-based approach is received with skepticism in the Global South,[41] where few countries wish to choose between China and the West. The US is moving towards decoupling digital hardware from China, yet Europe's position remains unclear, and developing countries may not side with Washington, if pressed.

CASE STUDY

HMN – CHINA'S SUBMARINE-CABLE CHAMPION

Submarine cables carry 99 percent of international data traffic. Chinese inroads into the sector have made cables part of China-US strategic competition.[42] China's HMN Technologies became the world's third-largest supplier of submarine cables in 2022.[43] The sector had for decades been dominated by the US's SubCom, Europe's Alcatel Submarine Networks (ASN) and Japan's NEC.

Fiber-optic cables have limited opportunity to increase market share by developing innovative or superior products. HMN's global rise has been fueled by state investment, affordable bank loans and bilateral agreements. In 2020, HMN submitted a bid 20 percent below that of competitors ASN and NEC for a project in Micronesia. The World Bank cancelled the bid after US lawmakers raised concerns about HMN building this link onto the US's HANTRU-1 cable.[44]

The US Senate Committee on Foreign Relations said Hengtong, which bought HMN from Huawei in 2020, may be involved in PLA military projects.[45] In December 2021, the US added HMN, Hengtong Marine Cable Systems and Hengtong Optoelectronics to its Entities List for acquiring or attempting to acquire US-origin items in support of China's military modernization.[46] Hengtong founder Cui Genliang has stated that his company leads in military-civil fusion.[47] The ex-army officer set up the private company in 1991, and he has been a delegate to the National People's Congress since 2012.

HMN and its parent company Hengtong are active worldwide. HMN builds the Pakistan & East Africa Connecting Europe cable (PEACE), which is part of China's Belt and Road Initiative. In Europe, it has built internet cables from Greece to Libya (Silphium) and from Sicily to Algeria (Hannibal).[48] An offshore power cable project in Portugal (WindFloat Atlantic) was led by Alcobre, a local firm 70 percent owned by Hengtong since

2015. Hengtong took majority stakes in Indonesia's Voksel, South Africa's Aberdare and Spain's Cablescom in 2015. In April 2023, Hengtong bought J-fiber, Germany's only manufacturer of high-end optical fiber.[49]

These activities are being challenged. The European Commission cited Hengtong in November 2021 as it put anti-dumping duties on Chinese optical-fiber cables.[50] Meanwhile, China is helping countries like Pakistan and Diibouti become less reliant on neighbors for digital infrastructure. HMN also benefits from vertical integration; unlike global competitors it often also serves as an operator.

Despite the trend towards block-building in the world of submarine cables, the risk of technical fragmentation remains low. The technology is relatively mature, so industry players rarely need to agree on new technical standards. However, it is possible US and EU regulators will take more steps to ban HMN from their networks or slow its growth, through non-technical requirements on public financing, transparency and cable ownership.[51]

Endnotes

1 | "The Discreet Power of China's Technical Standards," accessed November 7, 2022, https://shop.freiheit.org/#!/Publikation/1334.
2 | https://www.csis.org/analysis/will-ukraine-war-reshape-internet
3 | https://www.cnbc.com/2016/02/02/xiaomi-phones-were-on-sale-in-the-uswith-a-catch.html
4 | https://www.huaweicentral.com/huawei-tops-the-global-telecom-equipment-market-in-2021-delloro-group/
https://www.delloro.com/key-takeaways-2021-total-telecom-equipment-market/
5 | https://www.bloomberg.com/opinion/articles/2018-12-11/huawei-needs-emerging-markets-more-than-the-developed-world
6 | https://merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and
7 | https://eurasiantimes.com/beijing-to-discard-a-whopping-50m-computers-as-us-china-tech-wa/
8 | Operating CII comes with higher security responsibilities. The MLPS ranks any data handlers in five categories according to the exposure of the internet to their systems. Higher risk levels mean firms need to go through security review. https://www.china-briefing.com/news/critical-information-infrastructure-chinas-new-regulations/ , https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/, https://www.dataguidance.com/opinion/china-mlps-20-baseline-requirements-and-practical , https://www.samr.gov.cn/xw/tp/202211/t20221114_351626.html
9 | https://www.bloomberg.com/news/articles/2022-05-06/china-orders-government-state-firms-to-dump-foreign-pcs
10 | https://www.reuters.com/article/china-4g-licence-idUSL4N0JJ1VL20131204
11 | https://www.mobileworldlive.com/featured-content/home-banner/china-telecom-to-follow-hybrid-tdfdd-lte-path/
12 | https://simonlydeals.co.uk/4g-problems-chinese-smartphones/
13 | For example, the city of Jiangyan, not far from Shanghai, commissioned China Mobile Jiangsu to establish a City Administrative Service center. China Mobile then issued an open tender for Chinese companies to bid for this project.
14 | https://www.lightreading.com/mobile/4g-lte/report-huawei-zte-win-big-at-china-mobile/d/d-id/705369
15 | https://www.huaweicentral.com/huawei-claims-over-50-percent-of-5g-base-stations-in-china-report/
16 | Public procurement documents provided by ChinaFile.
17 | What is China's "National Cloud"? - by Zac Haluza (substack.com); https://cloudology.substack.com/p/what-is-chinas-national-cloud
18 | The Role of Cloud in China's Government Big Data System (substack.com): https://cloudology.substack.com/p/the-role-of-cloud-in-chinas-government
19 | Jonathan E. Hillman, The Digital Silk Road: China's Quest to Wire the World and Win the Future (New York: Harper Business, 2021). Chapter Five
20 | https://www.gov.cn/zhengce/content/202308/content_6898048.htm
21 | Hillman. Chapter Five
22 | https://www.americanprogress.org/article/solution-huawei-challenge/
23 | https://www.khmertimeskh.com/679345/officials-from-ministry-of-posts-and-telecommunications-of-cambodia-joined-5g-training-held-in-beijing-aiming-to-speed-up-cambodia-5g-launch-in-2020/
24 | http://finance.sina.com.cn/jjxw/2020-08-20/doc-iivhvpwy2017328.shtml, https://www.rferl.org/a/china-huawei-serbia-lobbyists-offshore/31531520.html, https://balkaninsight.com/2021/12/15/china-in-the-balkans-controversy-and-cost/
25 | https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/,
26 | What is China's "National Cloud"? - by Zac Haluza (substack.com): https://cloudology.substack.com/p/what-is-chinas-national-cloud
27 | Mapping Concentrations of Device Vendors in IXPs | RIPE Labs: https://labs.ripe.net/author/joao_m_ceron/mapping-concentrations-of-device-vendors-in-ixps/
28 | https://www.heritage.org/africa/commentary/how-china-has-been-using-huawei-made-cameras-spy-the-african-union-headquarters
29 | https://www.voachinese.com/a/huawei-latin-america/6452583.html; https://www.khmertimeskh.com/641998/with-huaweis-help-5g-in-cambodia-rolling-out-as-planned/; https://balkaninsight.com/2021/12/07/data-dominance-in-cyprus-a-chinese-outpost-inside-the-eu/; https://www.c114.com.cn/news/116/a1184717.html; https://balkaninsight.com/2021/12/15/china-in-the-balkans-controversy-and-cost/; http://finance.sina.com.cn/jjxw/2020-08-20/doc-iivh-vpwy2017328.shtml, https://www.c114.com.cn/news/116/a1184717.html; South Africa's Telkom launches 5G network with Huawei | Reuters: https://www.reuters.com/technology/south-africas-telkom-launches-5g-network-with-huawei-2022-10-27/; Huawei on a 5G roll in US ally Thailand – Asia Times: https://asiatimes.com/2022/01/huawei-on-a-5g-roll-in-us-ally-thailand/; https://tech.ifeng.com/c/8FJgtrn2WMw; http://uz.mofcom.gov.cn/article/jmxw/202210/20221003361256.shtml
30 | https://www.voachinese.com/a/huawei-latin-america/6452583.html
31 | French concern about Chinese Alibaba cloud for Paris 2024 (france24.com): https://www.france24.com/en/live-news/20211203-french-concern-about-chinese-alibaba-cloud-for-paris-2024
32 | https://tech.ifeng.com/c/8FJgtrn2WMw
33 | There Is a Solution to the Huawei Challenge - Center for American Progress: https://www.americanprogress.org/article/solution-huawei-challenge/

34| Lenovo founder in public backlash for 'unpatriotic 5G standards vote' · TechNode: https://technode.com/2018/05/16/lenovo-huawei-5g/
35| "The Discreet Power of China's Technical Standards."
36| Jonathan E. Hillman, The Digital Silk Road: China's Quest to Wire the World and Win the Future (New York: Harper Business, 2021).
37| Network effects: Europe's digital sovereignty in the Mediterranean – European Council on Foreign Relations (ecfr.eu): https://ecfr.eu/publication/network-effects-europes-digital-sovereignty-in-the-mediterranean/
38| Ericsson and Nokia are nearer to the endgame in China | Light Reading: https://www.lightreading.com/5g/ericsson-and-nokia-are-nearer-to-endgame-in-china/d/d-id/781282
39| https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1103
40| https://digitaldependence.eu/
41| The corresponding call for proposals is open only to EU entities, but they are encouraged to provide wholesale access to third parties, to include any kind of technology, and to subcontract parts to non-EU consortium members as long as non-discriminatory access is guaranteed Cf. Global Gateway: The EU Alternative to China's BRI – The Diplomat: Funding & tenders (europa.eu): https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2022-gateways-works;callCode=null;freeTextSearchKeyword=CEF-DIG-2022;matchWholeText=true;typeCodes=1,0;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destination=null;mission=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState; Cf. Global Gateway: The EU Alternative to China's BRI – The Diplomat: https://thediplomat.com/2021/09/global-gateway-the-eu-alternative-to-chinas-bri/
42| Hillary McGeachy "The changing strategic significance of submarine cables: old technology, new concerns" https://www.tandfonline.com/doi/abs/10.1080/10357718.2022.2051427
43| America's SubCom installed 118,000 km between 2018 and 2022, Europe's Alcatel Submarine Networks (ASN, owned by Nokia) 88,800 km, and HMN 55,700 km over the same period, overtaking Japan's NEC. https://subtelforum.com/products/submarine-telecoms-industry-report/
44| https://nypost.com/2021/06/18/pacific-undersea-cable-project-sinks-after-u-s-warns-against-chinese-bid/
45| https://www.foreign.senate.gov/imo/media/doc/SFRC_Majority_China_Europe_Report_FINAL_P_and_G.pdf
46| https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
47| http://www.hengtonggroup.com/index.php/xwzx/xwxq/1575.html; https://sinopsis.cz/en/arctic-digital-silk-road/
48| https://www.submarinecablemap.com/supplier/hmn-tech
49| https://cms.law/en/deu/news-information/cms-advises-hengtong-on-acquisition-of-leoni-owned-j-fiber; https://www.j-fiber.com/de/
50| https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R2011
51| https://ecfr.eu/publication/network-effects-europes-digital-sovereignty-in-the-mediterranean/

Conclusion
How to overcome European indecision in shaping the future internet

Conclusion
How to overcome European indecision in shaping the future internet

Our analysis has shown how China implements internet governance that is fundamentally different from that of Europe. Across data flows, web applications, internet protocols and digital hardware, China's vision and actions drive the fragmentation of the global internet. Occasionally it is also in Europe's interest to indicate disagreement with standards and norms that China seeks to organize global consensus for. That means that Europe does not pursue a unified global internet at all cost. Within this context, we suggest what we believe are the most optimal positions and actions for Europe. These suggestions are organized along the four layers, because the speed and shape of fragmentation is different in each of them, requiring unique strategies to enable European actors – governments, companies and others – to regain influence over the future of the internet.

1. DATA FLOWS

- **Demand regulatory clarity from Chinese authorities:** Beijing has recently retreated from stringent restrictions on cross-border data transfers. However, the scope of key concepts like "important data" needs to be made more transparent.

- **Prepare for added regulatory risk:** The national security-related considerations in China's regulatory regime challenge, in particular, firms in data-intensive sectors such as autonomous vehicles, pharma and intelligent manufacturing. They need to evaluate costs and benefits of their data strategies on the Chinese market, including ethical and reputational risks.

- **Prepare for worst-case scenarios:** Recent Chinese laws provide for retaliatory measures against actions by foreign governments, like for instance, China leveraging its data market for economic coercion and imposing tighter restrictions on access to the global internet.

- **Review ICT equipment and software applications originating from China:** The European Data Protection Board and the EU Agency for Cybersecurity could jointly establish a taskforce to get a better overview of tech firms headquartered in China that handle sensitive data in the EU, including both personal and non-personal data.

- **Foster trusted data coalitions:** To respond to the economic and political challenges emanating from China, the EU's cyber diplomacy needs to offer appealing propositions for digital economy and connectivity partnerships.

2. WEB APPLICATIONS

- **Monitor the global rollout of PRC-made mobile software platforms and coordinate responses within UN bodies like the Internet Governance Forum (IGF) and multi-stakeholder bodies like w3c:** Huawei's operating system is unlikely to compete with Android and iOS in developed economies, but it may do so in developing countries. Quick apps-type features could bring technical fragmentation there.

- **Review the EU's readiness for super-apps:** Existing regulation like the Digital Services Act (DSA) and Digital Markets Act (DMA) focus on US-based companies. The measures need to be reviewed to see how they can address challenges posed by Chinese products.

- **Call on China to improve foreign access to its online ecosystem:** Access and the open flow of information are increasingly difficult for businesses, diplomats, and researchers due to the use of pre-selected phone prefixes and geo-blocking. Privacy is at risk from real-name or phone-number registration.

- **Prepare for loss of access:** Stronger efforts are needed to preserve and archive online resources from the Chinese internet. Content is often available only briefly, or access is limited overall.

- **Inform the public about risks posed by using Chinese apps and websites:** Users joining Chinese platforms can become subject to Chinese laws and regulations, and they need to be familiarized with privacy risks of phone-number registration.

3. INTERNET PROTOCOLS

- **Coordination on technical language in standards development organizations:** Understanding China's often non-standard use of technical language requires expertise and time for a thorough analysis of Chinese proposals. Like-minded actors need to develop routines on how to swiftly coordinate during standard-setting conferences.

- **Compile a dictionary of Chinese technical terms:** Dedicated staff should look at Chinese domestic developments, because terminologies often appear first in domestic contexts before being used internationally.

- **Uphold a multi-stakeholder approach to maintain credibility:** Europe is drawing up a "fair share" contribution proposal for big tech platforms to contribute to developing digital infrastructure. The process for implementation has lacked transparency due to pressure from European telecommunications companies.

- **Invite diverse stakeholders to standardization bodies:** European governments should support SMEs, industry associations and NGOs in representing internet users' interests at standardization events.

4. DIGITAL HARDWARE

- **A consistent policy regarding Chinese hardware in European networks:** This is needed, especially as China obstructs European firms' access and Chinese laws are quite clear on companies needing to cooperate with security services. Europe should conduct a risk assessment, define "core networks" and "trustworthy vendors" and the possible risks of Chinese vendors, their impacts and likelihoods of these risks. A quantitative limit of 30 percent of hardware from any one country could be a possibility.

- **Ensure Europe has diverse vendors for hardware through regulation and financial incentives:** Network builders will struggle to stick to a 30 percent ceiling of components from one country in the short term as production is so concentrated.

- **Expand export credits to European vendors:** More support is needed for companies competing with big Chinese players like Huawei or HMN outside Europe.

- **Coordinate European positions in global standards-setting forums:** Governments should help improve the influence of European companies in global organizations. This needs a long-term strategy and research funding in areas like next-generation mobile internet standards.

- **Expand the EU's Digital Global Gateway:** The initiative needs more funds to become a real alternative to China's "Digital Silk Road". Network buildup in the Global South requires easy and swift access to funding, meaningful participation of local people and companies, and training for countries to operate networks themselves.

- **Maintain opportunities for constructive dialogue:** European country-agnostic measures provide a basis to call out China. At the same time, Europe needs to keep China involved in the global hardware layer alongside the US to prevent commercial and regulatory fragmentation from escalating into technical fragmentation.

Contributors

Kai von Carnap is an independent researcher. Until autumn 2023, he was an Analyst in the MERICS research team for Science, Technology and Innovation, focusing on the relation between the party state and information and communication technologies (ICTs) in the context of China's digital development path.

Antonia Hmaidi, Analyst, works on China's pursuit of tech self-reliance (especially in areas like semiconductors and operating systems), its internet infrastructure, and disinformation and hacking campaigns. Hmaidi also develops modelling and big data analysis tools.

Rebecca Arcesati, Lead Analyst, focuses on China's technology and digital policy as well as Europe-China innovation relations. She covers the global footprint of Chinese tech firms, digital infrastructure and surveillance tools, governance of data and artificial intelligence, technology transfer and research collaboration.

Jeroen Groenewegen-Lau, is Head of Program of "Science, Technology and Innovation" at MERICS. Prior to that he worked at "China Policy", a Beijing-based research and advisory company.

IMPRINT
MERICS | Mercator Institute for China Studies
Klosterstraße 64, 10179 Berlin, Germany
Tel.: +49 30 3440 999 0
Mail: info@merics.de
www.merics.de

EDITORIAL TEAM
Claudia Wessling, Director Communications and Publications, MERICS

Alexander Davey, Analyst and Editor, MERICS
Hannah Seidl, Communications and Publications Manager, MERICS

Mary Hennock, Freelance Editor
Ellen Thalman, Freelance Editor
Gerrit Wiesmann, Freelance Editor

DESIGN
STOCKMAR+WALTER Kommunikationsdesign

LAYOUT AND GRAPHICS
Alexandra Hinrichs, Graphic Designer, MERICS

The cover image was generated with the assistance of AI (Adobe Firefly).

Printed in Berlin, Germany

ISSN (Print): 2941-5799
ISSN (Online): 2941-5608