



HAL
open science

Global China in the Age of Algorithms

Séverine Arsène

► **To cite this version:**

Séverine Arsène. Global China in the Age of Algorithms. Maximilian Mayer; Emilian Kavalski; Marina Rudyak; Xin Zhang. Routledge Handbook on Global China, Routledge, 2024, 9781003044710. hal-04792313

HAL Id: hal-04792313

<https://hal.science/hal-04792313v1>

Submitted on 20 Nov 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Global China in the Age of Algorithms

Séverine Arsène

Manuscrit accepté par les éditeurs du projet de *Routledge Handbook on Global China*

INTRODUCTION: BIG DATA AS A MOMENT

It may be difficult to delineate clear boundaries of big data or artificial intelligence. This is about collecting large amounts of data points about any given phenomenon and computing it with various algorithmic methods. How much data qualifies as big data? What kinds of algorithms and computing techniques should be included?

From the standpoint of learning about Global China, these technical questions don't matter that much though. We can approach big data as a particular *moment* in the tech industry. It happened gradually at about the turn of the 2010s, when businesses and states identified big data as a strategic asset and started to act upon it when deciding on business plans and government priorities. This moment is as much a technological turn as it is an ideological one, when key economic and political actors are consumed with the belief that technology will inevitably change societies. As they work to make it happen, and to keep an upper hand on it, they enact somewhat of a techno-deterministic self-fulfilling prophecy.

This moment, this technological turn, played a key role in redefining China's place in globalization, precisely because of the fundamentally transnational nature of cutting-edge digital technology, and because of its strategic importance in China's ambition to be a leading technological power. In other terms, digital technology finds itself at the crossroads between globalization and techno-nationalism.

In this chapter I look at this conundrum, mostly by synthesizing and connecting recent literature from various disciplines: science and technology studies, anthropology, political economy, international relations and more. First, I examine how China emulated a global trend of betting on big data and used some of its specific assets to achieve the exceptionally fast and vast development of the digital industry. Secondly, I highlight how globalized and interdependent the technology sector is, from hardware to software and to labor. This means that the Chinese tech sector is deeply enmeshed in the global political economy, and a key stakeholder in global issues raised by tech development, from sustainability to labor and to ethical concerns. Thirdly, I show how China, the US and other countries have grown to see this interdependence as a liability in a context of increasing geopolitical tensions, and fourthly, how they took measures to "decouple", or to mitigate that perceived risk. In conclusion, I reflect on what that means for the global issues that China shares in common with the rest of the world, and which have not disappeared.

CHINA IN THE ERA OF ALGORITHMS

In his 2018 book *AI Superpowers*, Lee Kai-Fu, a China-based pioneer of artificial intelligence and influential opinion leader, predicted that "the invention of deep learning means that we are moving from the age of expertise to the age of data. Training successful deep-learning algorithms requires computing power, technical talent, and lots of data. But of those three, it is the volume of data that will be the most important going forward." (Lee, 2018: 12) This statement was in line with a commonly-held, though disputed, vision that "data is the new oil" (Arthur, 2013) and that it is fuelling a new industrial revolution with tremendous social and political impact. Lee believes that China will emerge as one of the most powerful players out of this.

Lee was not alone in thinking that big data, broadly defined, held the key to economic and technological dominance. By the end of the 2000s, tech companies around the world had made data collection a central part of their business, notably to refine advertisement and product recommendation, but also to repackage data into tradeable market knowledge. "When something online is free, you're the product", says the aphorism. Chinese tech giants made data a key part of their growth as well. Jack Ma, at the time CEO of Alibaba, famously said that Alibaba was not merely a retail company, but a data company.

Applications of big data-related technologies now range across vast domains of economic life across the whole country. Facial recognition technology enables identification of customers and securing online payments. Algorithms enable pattern recognition in very large amounts of data, with potential implications in health and medicine, environmental protection, education, and crowd management for instance. Automation of tasks also means that job markets could be affected massively within just a few decades. Of course, big data was also put to use in the fight against the Covid-19 pandemic (Pandaily, 2021).

The appetite for data entails abysmal paradoxes. In rural areas, for example, artificial intelligence is being applied by Chinese farms to combat food safety issues, in an attempt to control all parameters and predict outcomes of any event. Ever larger amounts of data are requested to make predictions accurate, but operating at larger scales generates ever more problems to solve (Wang, 2020: 84). Even then, public and private support for such technology is only picking up speed.

To support this trend, the Chinese government dedicated billions of RMB to the funding of AI-related research projects, and research centers (for instance via the China Academy of Sciences), and startups. It helps with adapted regulation and infrastructure, for instance by placing AI on Catalogues of Industries for Encouraging Foreign Investment (with favorable tariff policies and looser land use policies), and with the establishment of 8 "AI Innovation Zones" as of 2021 (Baruzzi, 2021).

Algorithmic government

The government gradually identified computing large amounts of data as a game changer in governance work too, and started building the necessary infrastructure, often in partnership with private companies. For example, in 2013 the "national bureau of statistics signed an agreement with 11 internet firms, incorporating the use of big data into government statistics" (Liu, 2021: 56). In 2015 a national data centre was built in Guizhou province, a relatively underdeveloped region now set to become the epicenter of Chinese big data.

In 2017, the State Council published a National Strategy for AI Development (State Council, 2017), indicating a clear ambition to lead the world in AI. It notably forecast an output of 1 trillion RMB for

the "core AI industry." AI is identified as a key economic engine, but also an important instrument to improve government work across all sectors including judicial services, medical care, and public security, thus ensuring social stability (Ding, 2018). Now, data and algorithms are at the centre of every significant public policy project, from smart cities to education and to the military (Kania, 2021).

Emulating a global trend

In some respects, the vision of an algorithmic society promoted by the CCP and big tech corporations is not particularly different from some of the promises made by techno-optimists elsewhere in the world, a trend sometimes criticized as "solutionism" (Morozov, 2013). In fact, Chinese leaders have long been inspired by American futurists and thought leaders like Alvin Toffler and Thomas Friedman, who chanted the advent of a fourth industrial revolution through digital networks as early as the 1980s (Gewirtz, 2019).

However, nowhere has this vision been deployed so fast and so vastly, both in the commercial and in the state sectors. The underdevelopment of telecommunication networks until the 1990s enabled China to "leapfrog" with the deployment of wireless technology across the territory. This facilitated the rapid adoption of smartphones and app-based ecosystems even in rural areas. Similarly, obstacles in the development of credit and credit card payments until the 2000s opened the way for e-commerce giants to fuel the rise in domestic consumption with dedicated mobile payment services, though often in a grey area of finance regulation. Free of the path dependency that characterizes many Western countries, and with enormous public and private investments, China's turn to digital technologies in all sectors of society has been spectacularly fast.

This was certainly facilitated by comparatively greater acceptance of such technologies among Chinese citizens. The World Values Survey shows that China is a global outlier, with higher positive views towards science and technology than most countries. It is also among the countries where surveillance is seen with a relatively positive eye (Fu, 2021). However, this seems to depend on circumstances and to be changing over time, as citizens are increasingly aware of privacy issues. For instance, in a 2021 survey "over 80% of respondents opposed the use of facial recognition in public spending places" (Wang, 2021).

For a long time, the fast development of digital technologies was also facilitated by a relative lack of regulation and tolerant policies. Few checks and balances enabled start-ups as well as tech giants to collect large datasets and experiment with algorithms in ways that would not have been permitted under a European or even American framework. This era seems to be coming to an end, as a wave of regulation is unfolding, with the Cybersecurity Law in 2017, a draft Data Security Law (National People's Congress, 2020a) and a draft Personal Information Protection Law in 2020 (National People's Congress, 2020b). In the winter of 2021, a vast campaign against anticompetitive practices also showed a signal that the industry would be under more scrutiny going forward.

Besides, Chinese corporations were encouraged to develop ethical standards (Roberts et al., 2019) (Arcesati, 2021). Corporate and public actors are active in studying and translating existing ethical standards developed in other countries, like the Asilomar AI Principles and the IEEE's Ethically Aligned Design report, for instance (Ding, 2018: 5).

Overall, China's foray into algorithms, and particularly artificial intelligence, has been impressive, but it remains difficult to assess whether China is really securing a dominating role in the field. A tentative "Capabilities" assessment conducted at the University of Oxford in 2018 concluded that China "trails the US in every driver except access to data" (Ding, 2018: 5). According to Li, Tong and

Xiao in the *Harvard Business Review* (2021), the strengths that helped China spring to its current position may also be long-term weaknesses, as future progress in AI will need much investment, especially in basic research, while China's strengths are more in applied science. In their view, the relaxed regulatory environment can also backfire, as some businesses are very cautious about stepping into sensitive fields like health data or into fields targeted in the trade war. O'Meara suggests in *Nature* that China still lacks "high-impact papers, people and ethics" (O'Meara, 2019).

Such assessments tend to reflect a view of China's technological rise in terms of great power competition, opposing China and the US in relatively binary terms. This view is shared across the board, including in China itself, where development plans do reflect a form of techno-nationalism that counts on leadership in the field of AI to establish China as a new great power. However, this view is in fact complicated by the inherent relationship of these technologies with globalization.

IN THE AGE OF ALGORITHMS, TECH IS INHERENTLY GLOBALIZED

Transnational flows

On the one side, the algorithmic turn of the tech industry in China has been a major contribution to China's economic growth and self-reliance, helping China rebalance an excessively export-led economy. The Great Firewall and other restrictions to foreign investments in telecommunications largely helped to shield Chinese corporations from foreign competition, and to develop a local digital ecosystem. Further to this, e-commerce and the platform economy, powered by algorithms, enhance domestic consumption, particularly in rural, remote areas (Luo, Wang & Zhang, 2019). This sector is a powerful engine in China's efforts to catch up with cutting edge technologies.

These achievements are not the product of an autarkic Chinese tech sector. On the contrary, China's digital technology sector is fundamentally enmeshed in the global economy.

First, supply chains are incredibly globally integrated. China produces 90% of global PCs and mobile phones (Woetzel et al., 2019: 63), and Chinese companies like Huawei and ZTE occupy an important place as global suppliers of telecommunication equipment. China needs to import large quantities of parts and intellectual property to fuel its technology industry, though this varies depending on the type of technology. For instance, over 50% of components of smartphones made in China, and over 65% of inputs in cloud services, are sourced from multinational players (Woetzel et al., 2019: 65).

China is also very globalized through transnational investment and finance. Even as there are limitations to foreign direct investment in the Chinese telecommunications sector, digital services still offer important investment opportunities for transnational finance. Many of the Chinese Internet giants are listed in the New York Stock Exchange, sometimes through workarounds like Variable Interest Entities. In 2014, Alibaba's \$25 billion IPO was deemed the largest in history. Even when not publicly listed, many of China's leading companies count international investors among their main shareholders, which also means that those institutions have a seat at the board (Jia & Ruan, 2020). Reciprocally, Chinese investors are eager to invest in companies in the US and in Europe, notably to access customer bases, marketing data or proprietary technologies. In 2017 before the trade wars, one could write "China's tech giants are pouring billions into US start-ups" (Fannin, 2017).

Indeed, intellectual property and innovation are essential to feed China's ambitions to lead in AI and digital technology. This requires high-skilled engineers and scientists, human resources best nurtured through international academic and business exchanges. For instance, many of the CEOs of China's unicorns hold a foreign advanced degree. Lee Kai-Fu himself is a notable example. Born in

Taiwan and trained in the US, he was an executive at Microsoft and Google before he became a prophet of China's domination in AI.

To accelerate this transfer of knowledge, and to limit potential brain drain, the Chinese government set up the Thousand Talents Plan, designed to enable Chinese-born scientists established abroad to settle in China, with generous funding and infrastructure at their disposal, as well as a Foreign Talents Plan for non-Chinese scientists (Zweig & Kang, 2020).

Meanwhile, many global companies **outsource** research and engineering jobs to China for cost-saving purposes and to get closer to the Chinese market. Zoom, for instance, is headquartered in the US but has product development teams in China (Kim, 2019). Most of the outsourcing happens at the lower end of the talent scale, though, as AI generates a boom in the data labelling business. Indeed, AI requires vast amounts of low-skilled labor to clean datasets and label information so that algorithms can "recognize" items in an image or calculate proper correlations. To fulfil this need, several "data annotations villages" emerged in rural areas (CAICT, 2020: 29). They often work for overseas customers, through crowdsourcing platforms like Amazon's Mechanical Turk, or perform tasks for AI firms in projects as diverse as autonomous driving and online ancestry services (Cadell, 2019).

Global issues

This embeddedness of the Chinese digital sector into global flows of goods, ideas and people means that China is a key stakeholder in some of the most pressing global issues today, which critical studies of technology have already highlighted, like labor conditions or sustainability.

The question of labor is often seen through the angle of automation replacing millions of workers. However, in the short term, a more pressing global issue revolves around working conditions of the millions of workers engaged in often invisible "digital labor." Chinese IT workers organized protest movements about the "996-ICU" work culture in the sector, denouncing a 9am-to-9pm workday, 6 days a week, leading some to the Intensive Care Unit. Such resistance of workers echoes other countries like the US, where tech workers protested in recent years against unfair treatment on the workplace or unethical projects (He & Shen, 2021: 11).

To conceptualize the global question of worker exploitation by transnational capitalist entities, Antonio Casilli talks about "coloniality" (Casilli, 2017). In *Goodbye iSlave*, Jack Qiu chooses even stronger terms, drawing our attention to the global alliance of Apple, the Taiwanese Foxconn and local Chinese governments to produce the very devices that keep us addicted to digital contents, on the back of millions of laborers whose working conditions are often edging closer to forced labor and displacement (Qiu, 2016). At a broader level, the extent of China's surveillance regime and the participation of tech companies inspires critical comparisons with "surveillance capitalism", a concept forged in the US (Zuboff, 2019). Indeed, Chinese tech is also subject to a movement of transnational financialization that has a taste for measuring humans' future preferences, based on today's behavioral data (Barclay, 2019). Even though each of these proposed conceptualizations lends itself to debate, this is a conversation worth having at a global level, considering that all actors are transnational in nature.

There is also, of course, the contribution of digital technology to global environmental issues. China has long been a major provider of Bitcoin mining, that consumes enormous amounts of electrical power, due to competitive energy pricing in certain provinces; and the country used to be a major importer of electronic waste. Even as such loopholes have been closed in recent years, this only prompted Chinese actors to expand operations overseas (Schulz, 2020).

Such important global issues would certainly warrant more active cooperation at the global level. In recent years, though, tech was much more often discussed under the lens of geopolitical competition.

GLOBALIZED TECH CREATE FRICTION IN A CONTEXT OF GEOPOLITICAL TENSIONS

Mutual dependency as vulnerability

In a context of increased geopolitical tensions, the mutual dependence between China and its foreign trade partners in the tech sector is increasingly seen by all actors as a dangerous liability. Many factors contributed to this, like the reinforcement of a tech-enabled authoritarianism in China, and the rise of populist politics in the US under the Trump presidency, both of which eroded mutual trust and enhanced a sense of competition for global domination. The centrality of digital technology in today's economic, political and social change all but enhanced the subject's sensitivity. Concerns range from strategic dependency over key industry assets, to potential spying and public opinion manipulation, and to ethical dilemmas faced by industry actors.

One issue is the dependency of the tech industry over assets mainly dominated by one country. Semiconductors have become a major point of concern for the Chinese government, as these are essential to the development of the tech industry, and particularly for the next generation of artificial intelligence and for 5G technology. There are chokepoints in the value chain, including technologies, equipment, and intellectual property, whereby Taiwanese, South Korean, US and European companies are in positions of oligopoly (Duchâtel 2021). China has been prioritizing investment in semiconductors in every policy document, but the most advanced technology requires so much investment and research that the task is daunting.

However, China also has a number of hard-to-replace assets, including its large-scale manufacturing capacity and know-how, which once got Tim Cook, Apple's CEO, to highlight that the tech sector does not choose China just for low wages anymore ("Apple's Tim Cook Tells Why Use China Manufacturing Capabilities", 2018). China's soil also produces about 80% of the world's rare earths, which are essential inputs into the manufacturing of electronic devices (Seaman, 2019).

Cross-border data flows

Moreover, **access to sensitive data** is also an important source of friction. Revelations by Edward Snowden in 2013 that the NSA had been massively spying on global telecommunication networks served to reinforce Chinese thought leaders' perception that cybersovereignty was of paramount importance (Arsène, 2016).

Meanwhile, Chinese digital corporations' intimate, though complex relationship with the Chinese Communist Party makes foreign governments wary of political risks. Since 2017, under the Chinese National Intelligence Law, businesses must comply with assistance requests from intelligence agencies (Dorfman, 2020). This forces foreign companies operating in China to make difficult choices about customer data security. It also encourages observers to believe that Chinese tech companies contribute data-processing capabilities to the Chinese party-state, to help it make sense of data obtained through murky channels, such as the 2015 hacking of the US Office of Personnel Management.

Even more importantly, there is growing concern about Chinese companies expanding in overseas markets. The asymmetry between the openness and loose regulation in Western markets, and protectionist policies on the Chinese market provide Chinese companies with opportunities to access sensitive data in client countries (Kokas, 2018). For example, there have been controversies about

potential uses of Huawei's networking devices to collect data. The 2020 TikTok standoff revolved mostly around two concerns: that TikTok could provide personal data from its wide user base in the US to its owner, the Chinese corporation ByteDance; and that it could influence American public opinion by censoring posts or by tweaking its recommendation algorithm at key moments such as elections (Ryan, Fritz & Impiombato, 2020).

There is indeed a form of extraterritoriality of Chinese censorship through users of Chinese social media platforms. Sometimes this works in unexpected ways. The Citizen Lab in Toronto showed, in two separate reports, that Wechat users registered in China continue to undergo censorship even after they transfer their accounts to Canada; and, even more intriguingly, that conversations between two overseas users of Wechat are subject to surveillance, and that files are used to train automatic censorship systems destined for Chinese users (Ng et al., 2016; Knockel et al., 2020).

As Liu Lizhi explains (Liu, 2021: 56), the very nature of data means that it is impossible for multinational corporations to completely alleviate these worries, because national regulation may force them to share personal data with their home government, and because datasets could stay for many years, meaning it is impossible to commit credibly not to repurpose it in ways that might encroach on civil liberties.

In fact, Chinese tech companies' appetite for foreign markets and investments is also of concern to the Chinese authorities. As cross-border data flows have now become a key focus of sovereignty concerns, information sharing obligations of listing abroad raise red flags for Chinese authorities. Didi, the monopolistic ride-hailing company, experienced it with the suspension of new downloads just 2 days after an IPO in New York (Yuan, 2021). More companies are likely to follow at the time of writing.

Ethical dilemmas

In the most sensitive areas, cross-border data flows generate acute ethical problems. The asymmetry of ethical norms and regulation between countries make cross-border arrangements in data management problematic. For example, applications of artificial intelligence in genomics could range from enhancing medical research to empowering ethnic discrimination and to advancing military objectives, with ethical red lines very difficult to draw. Advanced research in this field often involves cross-border exchange of expertise and datasets, for example with US researchers going to China to explore questions that they could not at home.

Issues with consent in data collection in China have led US scientific journals to revise their ethical guidelines, with some scientists calling for a stricter screening of articles from China. This is because ethical rules are impossible to enforce with certainty, and because of frequent involvement of police or military institutions in such research (Wee & Mozur, 2019).

In 2020, the genetics company BGI was put on a sanctions list by the US government for its role in "abusive DNA collection and analysis schemes to repress its citizens", referring mostly to DNA collection among the repressed Uyghur population. BGI's collaboration with the Chinese military also raises concerns. Besides, a 2021 Reuters report showed that the company repurposes genetic data from prenatal tests, including from overseas customers, and processes it using artificial intelligence methods to advance genomics research (Baldwin, 2021). This is also a sensitive topic for the Chinese authorities. In recent years, China started forbidding foreign researchers from working with Chinese genomic data.

Similar problems have arisen around other applications of artificial intelligence, such as facial recognition (Noorden, 2020), emotion recognition (which scientific basis are often weak) (Article 19, 2021), and public opinion measurement (Wu, 2020), all of which can have ethically problematic applications, such as abusive surveillance and discrimination.

DECOUPLING AND ITS LIMITS

Decoupling: Chinese and US measures

As a result of this increased focus on algorithms and data as strategic assets and as potential sources of vulnerability and conflict, states around the world have been encouraged to regulate the tech sector more conservatively, with state sovereignty and global competition in mind.

China has long had a very cautious approach to cross-border digital services, with the Great Firewall, policies supporting indigenous innovation, and limitations to foreign investments in the telecommunications sector. In the 2010s the country ramped up control even more, based on a consolidated doctrine on cybersovereignty. Beyond normative principles outlining states' sovereign rights in controlling contents, the Chinese regulator gradually focused more on securing the practical means of ensuring sovereignty, through "territorialization, indigenization, and investment" (Creemers, 2020: 8). This meant gradually reducing China's reliance on foreign technology and equipment, for instance by mandating administrations to source items from Chinese suppliers, or by subsidizing the industry, via such plans as Made in China 2025 and Internet Plus. As stated in policy documents, the overall intent is to make sure that networks are "autonomous and controllable" (Huotari et al., 2021).

A major milestone in this effort was the Cybersecurity Law, passed in 2017. It included mandatory security reviews and data localization requirements for "critical information infrastructures," a vaguely defined and broad category. Following this, the Cyberspace Administration of China published an avalanche of application measures, notably Guidelines for Data Cross-Border Transfer Security Assessment (2017), Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information, and Draft Measures for Data Security Management (both in 2019) (Liu, 2021: 52), among others. In April 2020, Measures for Cybersecurity Review were published, with a focus on supply chain security (Ross & Zhou, 2020).

In December 2020, the National Development and Reform Commission and the Ministry of Commerce jointly issued Measures for Security Review of Foreign Investment, with key information technologies as a clearly identified area of focus. Finally, in 2021, the National People's Congress promulgated the Data Security Law, to be implemented on September 1st, while a Personal Data Protection Law is in preparation.

Enforcement is also becoming more stringent, with recent high-standing cases, like severe sanctions on e-commerce giant Alibaba for anticompetitive practices, and placement of the ride-sharing company Didi under national security review. In both cases, investigations happened just before or just after a planned IPO in New York. As the companies list abroad, concerns arise about potential information sharing with foreign regulatory authorities and potential buyers. Business information, such as operation procedures or data collection practices, may be conceived by the Chinese state as important to national security. There is also concern about potential influence over strategic business decisions in a direction incompatible with Beijing's policy priorities.

Meanwhile, the United States also ramped up measures to reduce potential vulnerabilities in light of the US-China competition in technology, a trend that accelerated under the Trump administration

and in the context of the trade wars between China and the United States (see a list of measures in Rhodium Group 2021).

This included restrictions on foreign investment and trade in the United States. The powers of the Committee on Foreign Investment in the United States, which reviews business deals for national security concerns, were gradually strengthened. In 2018 Huawei, ZTE and other Chinese companies were excluded from public procurement of telecommunication services. Furthermore, the 2018 Export Control Reform Act listed artificial intelligence and data analytics among 14 broad “emerging technology” sectors under consideration for further export controls.

Separately, several companies were individually targeted with various forms of sanctions and exclusion from the American market, under a mix of trade, security, and human rights considerations. Between 2018 and 2020, the Bureau of Industry and Security under the US Department of Commerce added dozens of Chinese organizations on an Entities List which restricts export of US technology, including Huawei and chip manufacturer SMIC. In 2020, executive orders banned transactions with TikTok and Wechat on national security grounds, although this ban was contested in courts. The list goes on.

Restrictions also concerned human resources. In June 2020, the United States put several Chinese universities on the restricted entities list, like the Harbin Institute of Technology, thus preventing scientific partnerships. The US also revoked the visas of over 1000 Chinese students, who were considered at risk of transferring sensitive technologies to China.

Overall, the measures taken on both sides usually referred to as “decoupling”, bear high costs, notably in terms of disruption of technology supply chains, potential loss of future interoperability, and reduced cooperation between scientists and experts, as The US Chamber of Commerce warned in a report (Rhodium Group, 2021). Some rules enacted on both sides are incompatible, which could force transnational companies to withdraw from either market. For instance, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018 in the US, authorizes law enforcement agencies to compel US-based tech firms to hand over data, while the Cybersecurity Law in China mandates data localization, a conundrum for US service providers with customers in China (Liu, 2021). Overall, this decoupling movement, with trade wars as a background, represents great uncertainty for market actors, who have started lobbying against it (Rhodium Group & Covington, 2016).

Standards as a battlefield compatible with globalization?

Considering the high costs of a full-blown movement of deglobalization for all actors, and its detrimental role for tech development itself, risk-mitigating strategies are moving onto the international stage, with global negotiations over technical standards, in such institutions as the International Organization for Standardization, the Internet Engineering Task Force and many others. Standards can ensure interoperability of devices across markets, compatible security protocols, or recognition of personal data privacy, for instance. Pushing one standard over another can favor certain companies or states, depending on their access to proprietary technologies, on their specific objectives, and on their past choices of infrastructures. Therefore, standards emerged over the years as a key geopolitical battlefield (Seaman, 2020).

Historically, the world inherits American and European domination over global standards. In the early 2000s, attempts to mandate domestic standards on the Chinese territory were often unsuccessful, precisely because of the globalized character of high technology. There were conflicting interests between coalitions of industrial and policy actors eager to secure the domestic market on the one side, and corporations catering for global markets. The latter were not so

favourable to having to duplicate manufacturing arrangements for separate markets on the other side (Qiu, 2010; Ahmed & Weber, 2018).

A concerted effort by Chinese public and private actors to increase participation in global standardization organizations was much more successful, with Chinese engineers contributing an increasing proportion of technical work in key organizations (Arsène, 2015, 2021; Nanni, 2021). This makes rights defence organizations worried for future choices in terms of human rights. According to Article 19, "internationally, a head start on technical standards-setting could enable Chinese tech companies to develop interoperable systems and pool data, grow more globally competitive, lead international governance on AI safety and ethics, and obtain the 'right to speak' that Chinese representatives felt they lacked when technical standards for the Internet use were set." (Article 19, 2021: 14)

The Chinese leadership is also betting on trade partnerships to secure the expansion of tech markets, on China's terms. The Belt and Road initiative, including a digital Silk Road project, is part of this drive (see Creemers in this volume). Private initiatives complement this effort, like the eWTP project promoted by Alibaba and focused on developing countries. Branded as a "world trade organization for e-commerce", it is a logistics platform designed to help economic actors navigate trade barriers, regulation and financing hurdles (Harris, 2017).

The US and the European Union are also working to make a globalized tech landscape more compatible with their interests, with a view to keeping China's interests in check. That is the goal of the Clean Network project launched by the US. In the context of a disputed 5G rollout, the US rallied over 60 nations and 200 telecom companies around common principles. The European Union, meanwhile, is searching for a "third way", with regulatory steps like the General Data Protection regulation, and infrastructure projects like Gaia-X as a solution for "sovereign" cloud computing.

CONCLUSION

In the era of algorithms, big data and the algorithms used to process it have become essential instruments of China's economic development, facilitated by favorable policies, little path-dependency and a relatively welcoming user base. Despite the role of techno-nationalist policies and discourses in this trend, Chinese digital technologies are fundamentally enmeshed with globalized supply chains, circulation of intellectual property, and flows of human resources. It shares with the world some of the most pressing issues about economic growth, labor and ethics that large-scale data processing is raising.

However, in a context of rising geopolitical tensions, and under the influence of impulsive political styles, these interconnections have been increasingly seen as sources of vulnerabilities or, reciprocally, levers of pressure, by China, the US, and other global actors like the European Union. To mitigate such risks, a wave of "decoupling" measures was adopted in recent years, especially as heightened political tensions meant that political and economic costs weighted differently in the balance. This came at a great cost to the sector but with arguably limited effect in reducing global risks.

As more and more actors are coming to terms with the fact that global interconnections cannot (and, to some, it should not) completely be undone, the geopolitical competition is moving onto the global stage, in international organizations like the International Organization for Standardization, and in technical fora like the Internet Engineering Task Force. In fact, if anything, China doubled down on globalization during the last decade, through projects like the Belt and Road Initiative, which may enable the country to get global connectiveness on their own terms.

This means that although there is resistance to deglobalization, and critiques of protectionism and techno-nationalism abound, debates are overwhelmed by notions of geopolitical competition and rather binary worldviews. As He and Shen argue, "with its singular concern for utilitarian gains, [the great power competition narrative] risks equating technological advances and economic growth with societal well-being." It also "tends to underplay the transnational interests and struggles of social groups and classes impacted by innovation development and diffusion" (He and Shen 2021, 6-7), while leaderships lose sight of actual, broader well-being objectives.

Indeed, this competition tends to strengthen, rather than alleviate, long-term global sustainability issues. As countries focus on developing local digital champions, data hoarding is more likely to happen at the expense of privacy protection; intensive, low-cost labor is more likely to be exploited; natural resources are extracted in greater quantities; and global debates to address these issues are deprioritized. An important thing to watch will be whether future debates in standards setting are dominated by national interests or by a more global, long-term view of the public interest.

Bibliography

- Ahmed, S. & Weber, S. 2018. China's long game in techno-nationalism. *First Monday*. 23(5). DOI: 10.5210/fm.v22i5.8085.
- Apple's Tim Cook Tells Why Use China Manufacturing Capabilities*. 2018. Available: <https://idealmagnetsolutions.com/knowledge-base/apple-s-tim-cook-tells-why-use-china-mfg-capabilities/> [2021, July 06].
- Arcesati, R. 2021. *Lofty Principles, Conflicting Interests. AI ethics and governance in China*. Berlin: MERICS. Available: <https://merics.org/sites/default/files/2021-06/MERICSCChinaMonitor69AIEthics4.pdf>.
- Arsène, S. 2015. Internet Domain Names in China: Articulating Local Control with Global Connectivity. *China Perspectives*. (April):25–34.
- Arsène, S. 2016. Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order? *China Perspectives*. (2):25–36.
- Arsène, S. 2021. China, Information Technology and Global Freedom of Expression. A story of sovereignty and global capitalism. In *Regardless of Frontiers. Global Freedom of Expression in a Troubled World*. L. Bollinger & A. Callamard, Eds. New York: Columbia University Press.
- Arthur, C. 2013. *Tech giants may be huge, but nothing matches big data*. Available: <http://www.theguardian.com/technology/2013/aug/23/tech-giants-data> [2021, July 15].
- Article 19. 2021. *Emotional Entanglement: China's emotion recognition market and its implications for human rights*. London: Article 19. Available: <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>.
- Baldwin, K.N., Clare. 2021. Special Report: China's gene giant harvests data from millions of women. *Reuters*. 7 July. Available: <https://www.reuters.com/article/us-health-china-bgi-dna-idUSKCN2ED1A6> [2021, July 08].
- Barclay, B. 2019. *Is China becoming the world's most sophisticated surveillance regime?* Available: <https://www.thinkchina.sg/china-becoming-worlds-most-sophisticated-surveillance-regime> [2021, July 15].
- Baruzzi, S. 2021. *AI Innovation Zones in China: Opportunities for Foreign Investors*. Available: <https://www.china-briefing.com/news/ai-innovation-zones-in-china-opportunities-for-foreign-investors/> [2021, July 15].

- Cadell, C. 2019. Faces for cookware: data collection industry flourishes as China pursues AI ambitions. *Reuters*. 28 June. Available: <https://www.reuters.com/article/us-china-ai-data-insight-idUSKCN1TS3EA> [2021, June 28].
- CAICT. 2020. *Digital Economy Development in China (2020)*. Beijing: China Academy of Information and Communications Technology CAICT. Available: <http://www.caict.ac.cn/english/research/whitepapers/202007/P020200728343679920779.pdf> [2021, June 29].
- Casilli, A.A. 2017. Global Digital Culture| Digital Labor Studies Go Global: Toward a Digital Decolonial Turn. *International Journal of Communication*. 11(0):21.
- Creemers, R. 2020. *China's Conception of Cyber Sovereignty: Rhetoric and Realization*. (SSRN Scholarly Paper ID 3532421). Rochester, NY: Social Science Research Network. DOI: 10.2139/ssrn.3532421.
- Ding, J. 2018. *Deciphering China's AI Dream. The context, components, capabilities, and consequences of China's strategy to lead the world in AI*. Oxford: Future of Humanity Institute, University of Oxford. Available: https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.
- Dorfman, Z. 2020. Tech Giants Are Giving China a Vital Edge in Espionage. Available: <https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/> [2021, June 21].
- Fannin, R. 2017. *China's tech giants are pouring billions into US start-ups*. Available: <https://www.cnn.com/2017/03/08/chinas-tech-giants-are-pouring-billions-into-us-start-ups.html> [2021, June 28].
- Fu, Y. 2021. *Attitudes Towards Science, Technology, and Surveillance in 49 Countries · Yiqin Fu*. Available: <https://yiqinfu.github.io/posts/global-science-attitudes-2021/> [2021, June 22].
- Gewirtz, J. 2019. The Futurists of Beijing: Alvin Toffler, Zhao Ziyang, and China's "New Technological Revolution," 1979–1991. *The Journal of Asian Studies*. 78(1):115–140. DOI: 10.1017/S0021911818002619.
- Harris, D. 2017. What is eWTP, and why you should care. Available: <https://cargofacts.com/allposts/business/strategy/what-is-ewtp-and-why-you-should-care/> [2021, July 06].
- He, Y. & Shen, H. 2021. Beyond the Great Power Competition Narrative: Exploring Labor Politics and Resistance behind AI Innovation in China. *Georgetown Journal of Asian Affairs*. 7. Available: https://repository.library.georgetown.edu/bitstream/handle/10822/1061301/GJAA_He%20and%20Shen.pdf?sequence=1&isAllowed=y.
- Huotari, M., Gunter, J., Hayward, C., Zenglein, M.J., Lee, J., Arcesati, R., Meinhardt, R., Amela, E.C., et al. 2021. *Decoupling - Severed Ties and Patchwork Globalisation*. Available: <https://merics.org/en/report/decoupling-severed-ties-and-patchwork-globalisation> [2021, January 15].
- Jia, L. & Ruan, L. 2020. Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad. *Internet Policy Review*. 9(3):1–22. DOI: 10.14763/2020.3.1502.
- Kania, E.B. 2021. Artificial intelligence in China's revolution in military affairs. *Journal of Strategic Studies*. 0(0):1–28. DOI: 10.1080/01402390.2021.1894136.
- Kim, E. 2019. *Zoom, one of the most anticipated tech IPOs of the year, has one key profit driver: engineers in China*. Available: <https://www.cnn.com/2019/03/26/zoom-key-profit-driver-ahead-of-ipo-engineers-in-china.html> [2021, July 02].
- Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J.R. & Deibert, R. 2020. *We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*. Available: <https://citizenlab.ca/2020/05/we-chat-they-watch/> [2020, August 07].
- Kokas, A. 2018. Platform Patrol: China, the United States, and the Global Battle for Data Security. *The Journal of Asian Studies*. 77(4):923–933. DOI: 10.1017/S0021911818002541.

- Lee, K. 2018. *AI Superpowers. China, Silicon Valley and the new world order*. Boston: Houghton Mifflin.
- Li, D., Tong, T.W. & Xiao, Y. 2021. Is China Emerging as the Global Leader in AI? *Harvard Business Review*. (February, 18). Available: <https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai> [2021, June 23].
- Liu, L. 2021. The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*. 56(1):45–67. DOI: 10.1007/s12116-021-09319-8.
- Luo, X., Wang, Y. & Zhang, X. 2019. *E-Commerce Development and Household Consumption Growth in China*. (Policy Research Working Paper 8810). Washington DC: World Bank. Available: <https://openknowledge.worldbank.org/bitstream/handle/10986/31539/WPS8810.pdf?sequence=4&isAllowed=y> [2021, June 21].
- Morozov, E. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.
- Nanni, R. 2021. The ‘China’ question in mobile Internet standard-making: Insights from expert interviews. *Telecommunications Policy*. 45(6):102151. DOI: 10.1016/j.telpol.2021.102151.
- National People’s Congress. 2020a. *China’s “Data Security Law (Draft)”*. Translated by Emma Rafaelof, Rogier Creemers, Samm Sacks, Katharin Tai, Graham Webster, & Kevin Neville. Available: <http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/> [2020, July 15].
- National People’s Congress. 2020b. *Draft “Personal Information Protection Law”*. Translated by Rogier Creemers, Mingli Shi, Lauren Dudley, & Graham Webster. Available: <http://newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/> [2021, July 02].
- Ng, J.Q., Knockel, J., Ruan, L. & Crete-Nishihata, M. 2016. *One App, Two Systems: How WeChat uses one censorship policy in China and another internationally*. Available: <https://citizenlab.org/2016/11/wechat-china-censorship-one-app-two-systems/> [2016, December 01].
- Noorden, R.V. 2020. The ethical questions that haunt facial-recognition research. *Nature*. 587(7834):354–358. DOI: 10.1038/d41586-020-03187-3.
- O’Meara, S. 2019. Will China lead the world in AI by 2030? *Nature*. 572(7770):427–428. DOI: 10.1038/d41586-019-02360-7.
- Pandaily. 2021. COVID-19 Has Given China’s AI Industry a Shot in the Arm. Available: <https://pandaily.com/covid-19-has-given-chinas-ai-industry-a-shot-in-the-arm/> [2021, July 05].
- Qiu, J.L. 2010. Chinese Techno-Nationalism and Global Wifi Policy. In *Re-orienting Global Communication: Indian and Chinese Media Beyond Borders*. Chicago: University of Illinois Press. 284–303.
- Qiu, J.L. 2016. *Goodbye iSlave: A Manifesto for Digital Abolition*. University of Illinois Press. Available: <https://www.jstor.org/stable/10.5406/j.ctt1hfr0hz> [2020, January 12].
- Rhodium Group. 2021. *Understanding U.S. -China decoupling: Macro Trends and Industry Impacts*. China Center, U.S. Chamber of Commerce. Available: https://www.uschamber.com/sites/default/files/024001_us_china_decoupling_report_fin.pdf.
- Rhodium Group & Covington. 2016. *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*. Washington, D.C.: U.S. Chamber of Commerce. Available: https://www.uschamber.com/sites/default/files/documents/files/preventing_deglocalization_1.pdf [2017, August 15].
- Roberts, H., Cows, J., Morley, J., Taddeo, M., Wang, V. & Floridi, L. 2019. *The Chinese Approach to Artificial Intelligence: An Analysis of Policy and Regulation*. (SSRN Scholarly Paper ID 3469784). Rochester, NY: Social Science Research Network. Available: <https://papers.ssrn.com/abstract=3469784> [2019, December 10].
- Ross, L. & Zhou, K. 2020. *China Issues New Cybersecurity Review Measures*. Available: <https://www.jdsupra.com/legalnews/china-issues-new-cybersecurity-review-98878/> [2021, July 06].

Ryan, F., Fritz, A. & Impiombato, D. 2020. *TikTok and WeChat*. Available: <https://www.aspi.org.au/report/tiktok-and-wechat> [2020, September 15].

Schulz, Y. 2020. Chinese Engagement Abroad in the Scrap Business. *China Perspectives*. 2020(4):49–57. DOI: 10.4000/chinaperspectives.11225.

Seaman, J. 2019. *Rare Earths and China. A Review of Changing Criticality in the New Economy*. Paris: IFRI. Available: https://www.ifri.org/sites/default/files/atoms/files/seaman_rare_earths_china_2019.pdf [2021, July 06].

Seaman, J. 2020. *China and the New Geopolitics of Technical Standardization*. Paris: IFRI. Available: https://www.ifri.org/sites/default/files/atoms/files/seaman_china_standardization_2020.pdf.

State Council. 2017. *China's "New Generation Artificial Intelligence Development Plan" (2017)*. Translated by Graham Webster, Rogier Creemers, Paul Triolo, & Elsa B. Kania. Available: <http://newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> [2021, June 23].

Wang, C. 2021. *Report on the Abuses of Facial Recognition Technology 人脸识别技术滥用行为报告*. Translated by Jeffrey Ding. Available: https://docs.google.com/document/u/1/d/1rWoqdwT6a52kO2Q-QVPfHdbtyoS8RkaWls5hbZRLB2M/edit?usp=sharing&usp=embed_facebook [2021, June 22].

Wang, X. 2020. *Blockchain Chicken Farm*. McMillan, Farrar, Straus and Giroux. Available: <https://us.macmillan.com/blockchainchickenfarm/xiaoweiwang/9780374538668> [2020, June 18].

Wee, S.-L. & Mozur, P. 2019. China's Genetic Research on Ethnic Minorities Sets Off Science Backlash. *The New York Times*. 4 December. Available: <https://www.nytimes.com/2019/12/04/business/china-dna-science-surveillance.html> [2020, April 18].

Woetzel, J., Seong, J., Leung, N., Ngal, J., Manyika, J., Madgavkar, A., Lund, S. & Mironenko, A. 2019. *China and the world: Inside the dynamics of a changing relationship*. McKinsey Global Institute. Available: <https://www.mckinsey.com/~media/McKinsey/Featured%20Insights/China/China%20and%20the%20world%20Inside%20the%20dynamics%20of%20a%20changing%20relationship/MGI-China-and-the-world-Full-report-June-2019-vF.ashx>.

Wu, A.X. 2020. Chinese Computing and Computing China as Global Knowledge Production [Special Section]. *Catalyst: Feminism, Theory, Technoscience*. 6(2). DOI: 10.28968/cftt.v6i2.34363.

Yuan, L. 2021. For China's Business Elites, Staying Out of Politics Is No Longer an Option. *The New York Times*. 6 July. Available: <https://www.nytimes.com/2021/07/06/technology/china-business-politics-didi.html> [2021, July 07].

Zuboff, S. 2019. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord: Profile Books.

Zweig, D. & Kang, S. 2020. *America Challenges China's National Talent Programs*. (4). Washington DC: CSIS.