MERICS
**PAPERS
ON CHINA**

CHINA'S DIGITAL RISE

Challenges for Europe

Kristin Shi-Kupfer | **Mareike Ohlberg**

No 7 | **April 2019**

merics
Mercator Institute
for China Studies

CHINA'S DIGITAL RISE

Challenges for Europe

Kristin Shi-Kupfer | **Mareike Ohlberg**

Content

Exhibits:

Acknowledgements

This study would have been impossible to undertake and accomplish without the support by a great number of experts and colleagues. It is based on a foresight paper that was commissioned by the European Political Strategy Centre, European Commission, in autumn 2018.

This study has profited greatly from the encouragement and feedback of leading international experts in China's digitalization. We would especially like to thank participants of a workshop on scenarios of China’s digital futures at MERICS with experts from government, industry, and think tanks in October 2018 on the issue of “How will China impact the digital environment in Europe in 2030?” We thank Nabil Alsabah (Bitkom e.V.), Séverine Arsène (The University of Hong Kong), Luís Viegas Cardoso (European Political Strategy Centre), Svenja Falk (Accenture Research), Hauke Gierow (G DATA Software), Helmut Kranzmaier (Infinitec), Qin Liwen (Trends Eurasia), Fanny Ries (Federal Ministry of Defense) and our MERICS colleagues for contributing to the workshop on October 2, 2018.

We are very grateful for our colleagues Yishu Mao, Anna Holzmann and Helena Legarda who contributed research and also drafted parts of this study. A very special thank you goes to former MERICS Visiting Fellow Samantha Hoffman who brought in her great expertise.

We would like to acknowledge the very helpful research support of Felix Turbanisch and Kai von Carnap.

Our special gratitude goes to the MERICS publications team, namely Claudia Wessling, Alexandra Hinrichs and Mary Hennock, for their extensive support in improving and producing this study and the communications team for getting out the word.

We are greatly indebted to our colleagues Mikko Huotari, the Deputy Director of MERICS, and Jan Weidenfeld, Head of European Affairs and Business Strategy, who have helped enormously to shape and refine this study.

While all the people mentioned above helped to improve this report, the authors bear sole responsibility for any remaining errors.

Kristin Shi-Kupfer and Mareike Ohlberg

Berlin, April 2019

Executive Summary

CHINA'S BOLD AMBITIONS TO LEAD IN DIGITAL TECHNOLOGIES POSE CHALLENGES TO EUROPE

- China is making headway in achieving global leadership in 5G, AI and quantum computing and in other digital and disruptive technologies
- The Chinese Communist Party (CCP) is pursuing a comprehensive digital strategy encompassing the search for new economic growth drivers, cyber governance and global power projection
- Selected leading Chinese ICT companies are co-shaping the global digital architecture
- With its proactive approach to standardization, China sets operational rules for foreign businesses
- China's weak regulatory environment will impact on the development of digital ethics on a global level

The reach of Chinese IT companies into global digital infrastructure is raising growing concerns in Europe. Large and partially state-backed companies like Huawei, Alibaba or Tencent are already involved Europe-wide in telecommunications networks, data centers and online payment systems. The introduction of the new telecommunications standard 5G will likely contribute to Huawei's hard- and software becoming yet more entangled in Europe's critical infrastructure. China is the only country that is ahead of the UN's International Telecommunication Union's "2020 5G development schedule". Chinese experts have taken the lead role in the 5G group of the International Standardization Organization (ISO), known as 3GPP, by submitting 40 percent of the standards and 32 percent of the documents.

The global leadership of Chinese telecoms giants in 5G is just one example of how China is on its way to becoming a digital innovation powerhouse. President Xi Jinping has emphasized the importance of China becoming a leader in emerging technologies – including artificial intelligence (AI), nanotechnology, quantum computing, big data, cloud computing, and smart cities. China has spent at least ten times more on quantum R&D than the United States; estimates start from USD 50 billion. In the AI sector, China filed 30,000 patents in 2018 alone, 2.5 times more than the United States. China has also announced plans to invest USD 411 billion in upgrading its telecommunications systems to 5G between 2020 and 2030.

China is well on its way to being a global leader in key emerging and digital technologies. It is a leading digital marketplace and home of one third of unicorns, privately held start-up companies valued at over USD 1 billion. China has made substantial headway in AI-based applications like facial recognition, in blockchain technologies and quantum computation. It has achieved substantial growth across multiple other sectors, such as logistics, e-commerce, fintech, autonomous driving, and digital health.

And Chinese companies are competing successfully worldwide in ICT products and services. Beijing is proactively shaping international standards for emerging technologies including blockchain, Internet of Things (IoT) and 5G, by securing leadership positions in international standard setting bodies.

For Europe, the loss of economic competitiveness in these fields is becoming a pressing concern. At the same time, the fact that Chinese high-tech enterprises are gradually conquering European markets and their digital technologies are increasingly found in fintech, e-commerce and telecoms structures in Europe feeds into worries over potential security risks. The ongoing transfer of dual-use technologies from Europe to China adds to these concerns.

CHINA'S DIGITAL AMBITIONS ARE BACKED BY STRONG POLICY COORDINATION AND A NEXUS OF PARTY STATE AND PRIVATE INTERESTS

China's digital strategy covers its entire economy and society. It envisions rapid technological advances to generate fresh economic growth, foster effective governance and control, and project global power. The strategy combines economic targets with broader normative and security goals. The Chinese Communist Party (CCP) wants to advance technologically, amplify China's "discursive power" and shape global standards and norms.

Multiple major policy initiatives support these goals: the National Informatization Strategy (2016 – 2020) calls upon China's internet companies to "go out" into the world and support the creation of a "Digital Silk Road". The "Made in China 2025" roadmap and "Internet Plus" were launched in 2015 to drive domestic industrial and digital innovation. The digital sector has been a major beneficiary of President Xi's policy style, which relies on task-specific Leading Small Groups to quickly implement decisions made by the top leadership in sectors that are considered a priority.

On the ground, a unique party-state-private nexus in the ICT sector underpins China's digital policies. The CCP has nurtured the home-grown IT champions Baidu, Alibaba and Tencent (known as "BAT") by blocking foreign competitors from the domestic market. The party state also allowed BAT to expand internationally and to access foreign capital with listings on overseas stock markets. In the case of ZTE and Huawei, the two major Chinese telecommunication equipment manufacturing companies, party-state co-optation in the form of government funding and preferential procurement has been particularly evident. It can be hard-to-impossible to track the web of party influence, state control mechanisms and international linkages that surrounds China's sprawling ecosystem of innovative start-ups, venture capital funds, local and provincial governments – and the military.

China enjoys structural advantages in advancing its bold plans to digitize the economy and achieve global technological leadership. Beijing channels massive amounts of capital through state guidance funds into emerging technologies. In line with the unofficial slogan "First develop, then regulate," the government enables commercial actors to innovate and swiftly produce market-ready products for a digital ecosystem protected from foreign competition.

China is investing heavily in different areas of technological innovation: For instance, training new talent is a prioritized sphere of action. In AI, China intends to establish at least 50 academic and research institutes by 2020. China's government hopes to gain substantial economic benefits by pushing digital innovation within and beyond its borders: for instance, it is estimated that products and developments for the Internet of Things (IoT) alone could add up to 1.8 trillion USD in cumulative GDP growth for China by 2030.

However, China's digital strategy should not be viewed as a purely economic exercise. Civil-military integration has been a top-level national strategy since 2014. Efforts to become a "science and tech superpower" should be seen in close connection with ambitions to dominate in emerging dual-use technologies, advance cyber warfare capabilities, weaponize AI and achieve quantum supremacy.

UTILIZING DIGITAL INNOVATION FOR POLITICAL AND SOCIETAL CONTROL

China's drive for digitalization goes beyond economic ambitions: Beijing wants to use digital technologies for effective governance and control over companies and citizens. It is focusing on two main goals:

a) protecting critical infrastructure and data from foreign access, and
b) establishing big data-based control mechanisms to monitor enterprises and citizens in order to enforce compliant and conformist behavior.

The CCP has invented powerful tools to pursue its vision of cyber governance, social management and control. The Cyber Security Law, effective since July 2017, regulates the protection of IT infrastructure and systems, data management for public services, and governs the regulatory compliance of economic and societal actors. Access for foreign companies to China's digital and telecommunications markets will remain restricted due to informal barriers created by strict regulations on cyber and data security.

Plans to introduce a nationwide "Social Credit System" (SoCs), a big data-fueled toolkit to enforce laws, regulations, or party-state targets by scoring companies and individuals, are progressing. Currently, they consist of more than 40 fragmented local government SoCs pilot programs and numerous commercial pilots set up by technology firms. However, they could become a powerful and comprehensive instrument to steer the behavior of citizens and organizations.

WEAKNESSES IN CHINA'S APPROACH

Despite the structural advantages described above, China's digitalization strategy faces multiple internal and external challenges that could derail its ambitions. Internally, conflicting goals and stakeholder interests create substantial tensions. Heightened party control over private companies and inefficient allocation of capital may ultimately also come at the expense of innovation. China will still depend on foreign core technologies in the years to come. This became apparent last year, when ZTE almost went bankrupt after the United States threatened a ban on selling microchips to the telecommunications supplier.

More broadly, Beijing's industrial and technology policies, as well as digital-related laws and regulations such as the Cyber Security Law are increasingly putting China in conflict with other international actors, in particular the United States. The global backlash against China's digital and technological rise has probably only just begun.

In spite of these challenges, China will pursue its drive for digital innovation and leadership. China's leaders view achieving leadership of global technological progress as a political project charged with nationalist and ideological significance.

CHINA'S DIGITAL POLICIES PUT PRESSURE ON EUROPE

China's digital ambitions already have an impact on Europe's politics, economics, and security. The "Digital Silk Road" is likely to deepen China's digital reach into Europe. Going forward, the EU faces the growing commercial presence of, and critical dependence on, China's most competitive IT players. IP protection in research collaborations and other new regulatory challenges in managing interlinked digital markets will emerge as major challenges going forward.

In cyber security, the EU is confronted with a direct challenge from China's digital outreach. European companies and government bodies have suffered commercial espionage and cyber-crime originating from Chinese institutions. The growing presence of major Chinese ICT suppliers including Huawei and ZTE creates substantial uncertainties and potential security risks for EU member states.

China's growing digital reach is likely to have more direct negative consequences for European politics and core values. Many aspects of China's social credit system run counter to the EU's values, including the lack of privacy protection and freedom of expression, and to EU efforts to establish digital ethics standards. European citizens' privacy, safety and rights need protection from Chinese government encroachment and – by extension – from commercial actors who could collect and use data on EU citizens and others within EU territory.

China's high-tech rise is not a threat to the EU per se: if innovation were based on reciprocal and transparent cooperation, transcending protectionist logic, all sides could benefit from new ideas and developments. But if China pursues a path of self-reliance this will pose fundamental challenges to co-operation and mutual confidence. The EU's current lack of a truly European innovation eco-system and its politically inconsistent responses to China suggest it will struggle to cope.

European decision-makers need to prevent a worst-case scenario in which a fragmented EU faces a digitally aggressive China competing with the US in a fragmented digital global economy. An immediate concern should be how the EU manages transatlantic relations in such as context, i.e., how European governments deal with the lure of economic opportunities related to China's digital transformation in a situation where the United States anticipates this space as crucial for strategic competition with China.

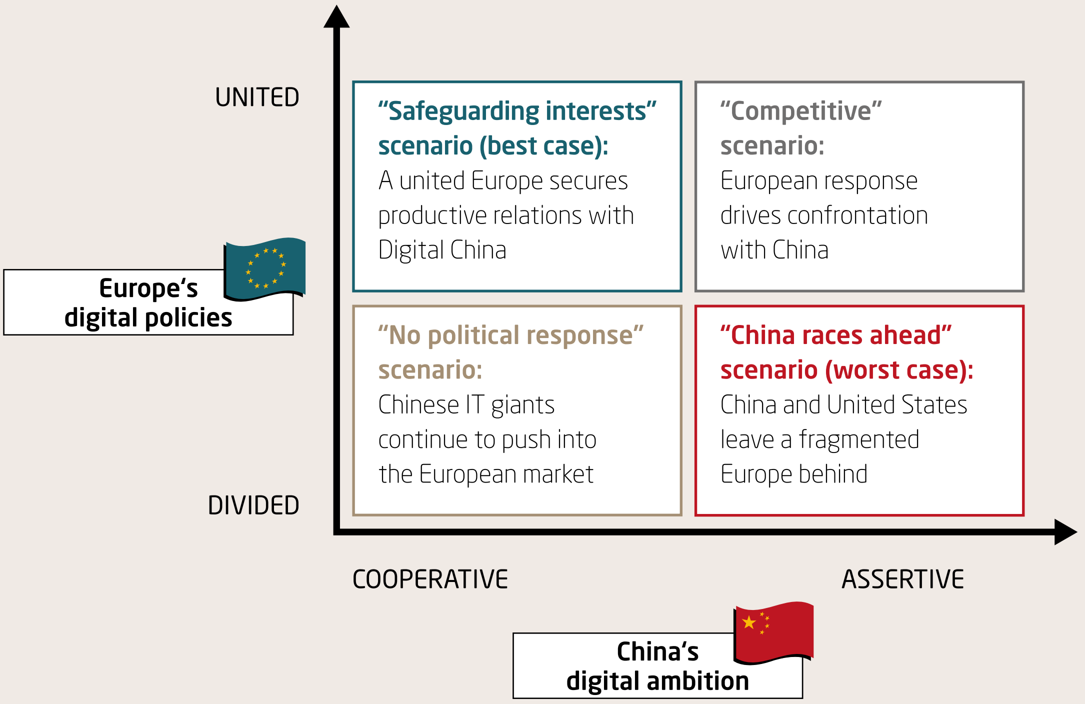
Unless Europe catches up and becomes competitive in key digital technologies, it faces an imminent risk of finding itself trapped between China and the United States. The EU and its member states need to join forces to prioritize strengthening the European digital market, by developing secure supply-chains among trusted partners for core digital technologies and devising strategically effective and autonomous digital policies.

Digital China is challenging Europe on several levels. Opportunities for collaboration exist, however, Europe needs to safeguard its interests in a fast changing economic and technological environment. European policy makers need to double down on developing a strategically autonomous, unified digital policy and strive for a joint approach in tackling cyber security issues in Europe.

Facing China's digital rise, Europe needs to seek greater alignment with third countries like the United States, South Korea or Japan in pushing back jointly against China's subsidized industrial policy and its emphasis on indigenous innovation that fosters digital protectionism. Europe also needs to rapidly expand work with like-minded partners towards agreements on privacy, data localization and cyber standards, as well as free and safe data flows. Vigilance, unity and leverage will be needed to prevail in a digital world that is increasingly shaped by China.

China's digital rise will affect Europe

A look into possible future trajectories



"Safeguarding interests" scenario (best case): A united Europe secures productive relations with Digital China

"Competitive" scenario: European response drives confrontation with China

"No political response" scenario: Chinese IT giants continue to push into the European market

"China races ahead" scenario (worst case): China and United States leave a fragmented Europe behind

Source: MERICS

© MERICS

1. Introduction: Digital China goes global

Huawei, the Chinese telecommunications company that recently has been the focus of controversial discussions in many industrialized countries, embodies like no other the global rise of Digital China: Nurtured at home by the Communist Party (CCP), Huawei set out to expand into overseas markets. From 2014 to 2018, Huawei more than doubled its revenues to reach 108 billion USD. This tremendous growth was mostly driven by gains in foreign markets. In 2017, the company overtook Ericsson and now owns the largest global market share in mobile infrastructure equipment. In 2018, Huawei became number one in global sales of mobile phones, beating Apple.[1] The English translation of "Huawei" (华为) indicates that the company's success story also serves as a national blueprint: "China (hua) is able (wei)."

China's ambition to become a leader in digital technologies in general is driven by both political and economic motives: for the CCP, the digital age offers a chance to restore China to its perceived "rightful place" in the global order. According to official party history, China led the world in scientific and technological innovation for centuries. After Europe's Industrial Revolution, China was semi-colonialized, beginning a 'Century of Humiliation' that ended only with the CCP's victory in 1949. Now the CCP hopes to turn the tables and restore its former glory by a technological revolution powered by Artificial Intelligence (AI) and other digital technologies.

For the CCP, the digital age offers a chance to restore China to its "rightful place" in the global order

The CCP's legitimacy rests heavily on economic performance; stagnating or even declining growth poses a serious risk to its grip on power. All-encompassing digitalization is considered essential for the ambitious economic modernization agenda that aims at upgrading China from the "workshop of the world" into a high-tech leader with globally attractive innovative products and services, and modernized manufacturing processes.

Digitalization goals feature prominently in China's macro-economic planning and are at the core of its ambitious industrial and technology policy planning. Macro-economic plans are complemented by more concrete and technology-specific plans that lay out specific policy measures, time tables and implementation targets, for instance on AI, Cloud Computing, and Big Data.[2] The Made in China 2025 strategy (MiC 2025) of May 2015 is the most comprehensive industrial policy plan to date for 10 core industries: in it, the State Council puts strong emphasis on smart manufacturing to usher in the digital transformation of industry.[3] An update of the "roadmap" for this strategy in early 2017 doubles down on self-reliance for core emerging technologies and global leadership ambitions (see exhibit 1).

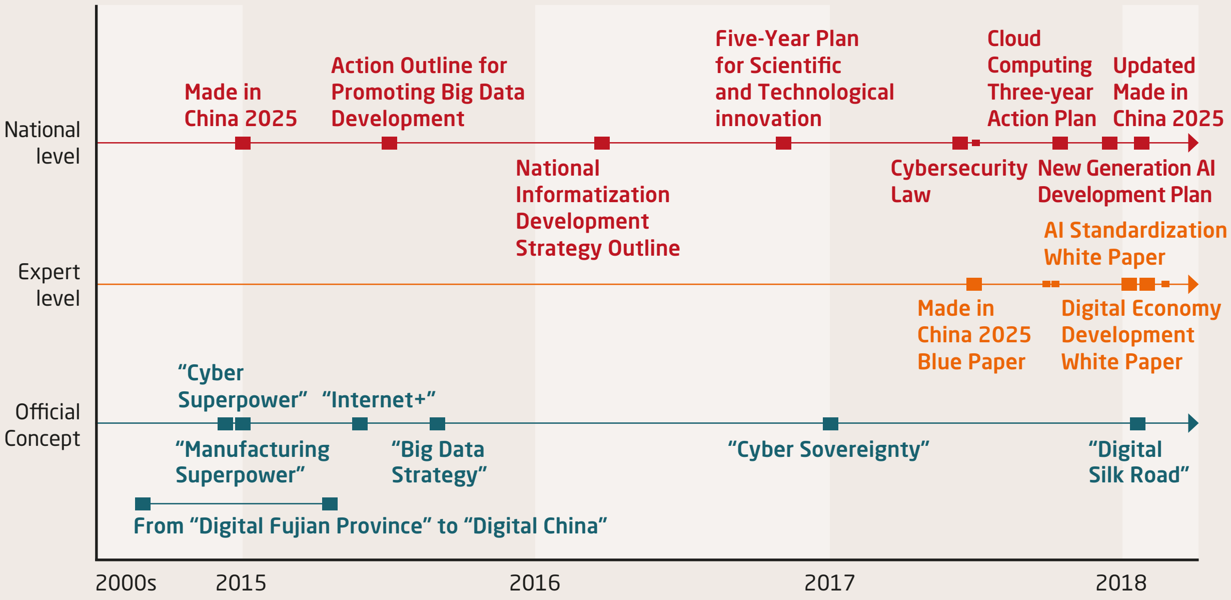
However, China's digital ambitions should not be viewed as purely economic or civilian exercises. They combine economic goals with broader normative and security aims. To achieve "great national rejuvenation," the CCP wants China to advance technologically while simultaneously amplifying what the party-state calls "discursive power" (话语权) by shaping global standards and norms. At the same time, civil-military integration has been a top-level national strategy since 2014, and China wants to dominate emerging digital dual-use technologies to advance its high-tech military capabilities.[4]

China's digital ambitions have an impact far beyond its geographical borders; its digital products and services are already conquering global markets. It is also seeking global digital leadership in multiple other ways, spearheading international initiatives around digital infrastructure, e-commerce, and research collaboration.

Exhibit 1

The making of China's digital ambitions

Overview of key policy initiatives



Source: MERICS

© MERICS

Within the framework of the so-called Digital Silkroad, China has initiated major digital infrastructure projects, e.g. building cable networks connecting Asia and Europe overland. The country has also made headway towards shaping international standards for emerging technologies by fostering industry participation as well as securing leadership positions in international standard setting bodies. As a result, China is now in a leading position on the standardization of blockchain technology, 5G and the Internet of Things (IoT).

China's digital ambitions are likely to threaten core European values such as privacy or freedom of expression

For Europe, there are opportunities and serious challenges. China's digital IT champions are competing – often unfairly – in European digital markets selling a wide-range of subsidized products and services. IP protection in research cooperation and regulatory challenges around data privacy are pressing issues. The EU also faces substantial security risks of cybercrime and espionage related to China-originated components and infrastructure. In future, China's digital ambitions are likely to threaten core European values such as privacy or freedom of expression. Only if the EU and the individual member states align themselves to promote European technologies and a single digital market as well as take stricter measures to protect citizens and crucial infrastructure, will the continent potentially become capable of mitigating challenges from China's digital rise.

2. China is building up digital leadership at home and abroad

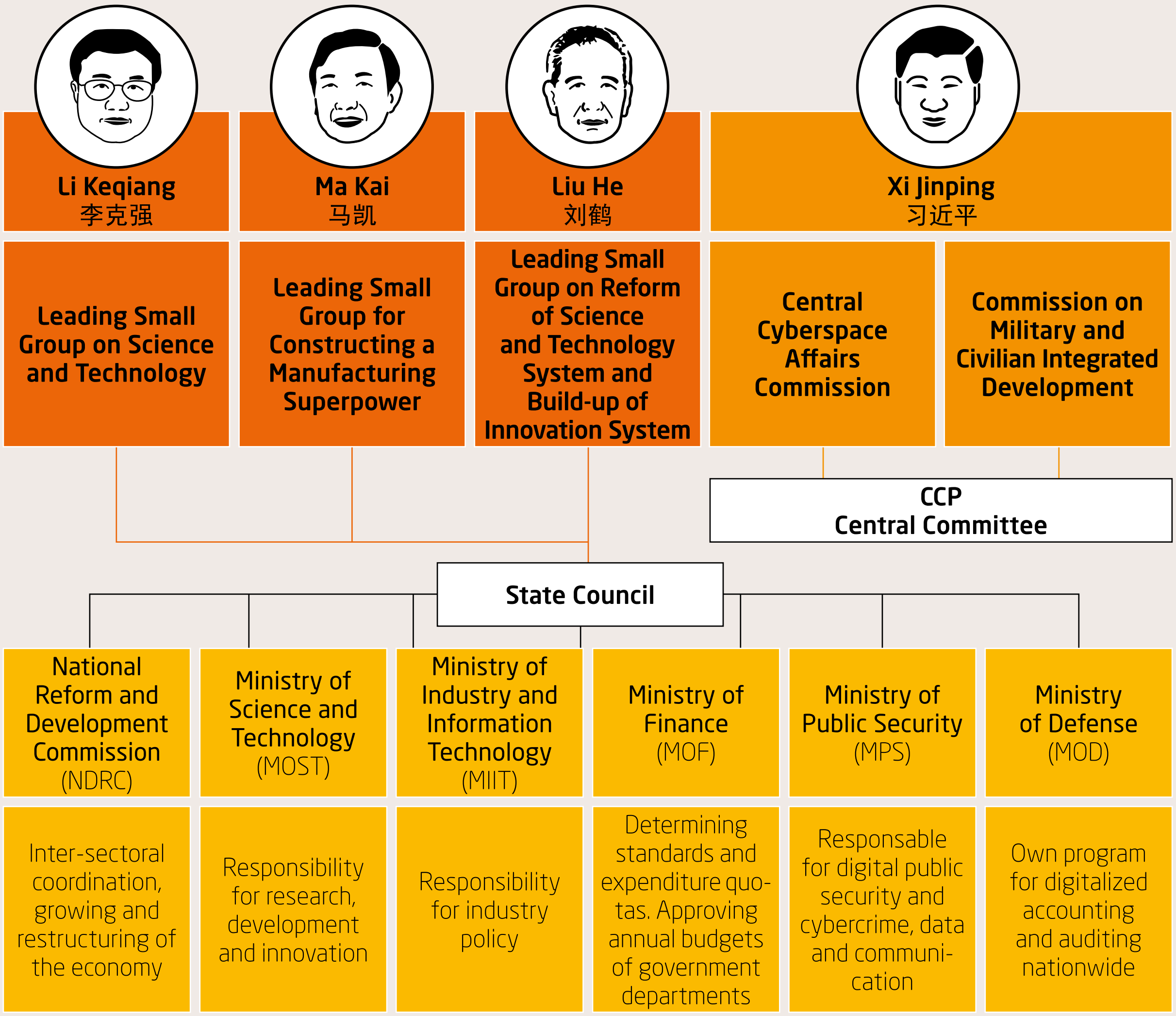
The People's Republic of China's (PRC) ambitious digital strategy spans all areas of economy and society and combines major domestic and international projects. To achieve macro-economic and social re-engineering, the CCP under Xi Jinping is building on two distinctive aspects of its political economy: 'top-level policy design' (顶层设计) and a unique private-party-state nexus in the ICT sector.

To ensure that decisions made at the top are swiftly conveyed to lower, executive levels, the Xi government and the CCP rely on so-called 'leading small groups' and commissions for coordination. Two of these groups, on Cyberspace Affairs and Military Civilian Integrated Development, were recently upgraded to Central Commissions, which empowered them to better coordinate and enforce the implementation of digital policies (see exhibit 2).

Exhibit 2

Multiple interests need constant coordination

The makers of China's digital policies



Li Keqiang
李克强

Ma Kai
马凯

Liu He
刘鹤

Xi Jinping
习近平

Leading Small Group on Science and Technology

Leading Small Group for Constructing a Manufacturing Superpower

Leading Small Group on Reform of Science and Technology System and Build-up of Innovation System

Central Cyberspace Affairs Commission

Commission on Military and Civilian Integrated Development

CCP
Central Committee

State Council

National Reform and Development Commission (NDRC)

Ministry of Science and Technology (MOST)

Ministry of Industry and Information Technology (MIIT)

Ministry of Finance (MOF)

Ministry of Public Security (MPS)

Ministry of Defense (MOD)

Inter-sectoral coordination, growing and restructuring of the economy

Responsibility for research, development and innovation

Responsibility for industry policy

Determining standards and expenditure quotas. Approving annual budgets of government departments

Responsable for digital public security and cybercrime, data and communication

Own program for digitalized accounting and auditing nationwide

Source: MERICS

© MERICS

The CCP has also systematically fostered different forms of private-state-party collaboration in the ICT sector. It supported domestic IT champions like Baidu, Alibaba or Tencent by blocking foreign competitors from the Chinese market. The party-state allowed these companies, which nowadays also go by the acronym BAT, to get listed on overseas' stock markets, access foreign capital and to expand their business into other markets. At the same time, the CCP deploys fairly effective mechanisms to control and steer these internationally networked companies.

Other means of party-state co-optation include support from the government through funding and preferential procurement, as is the case for the two major Chinese telecommunication equipment manufacturing companies, ZTE (officially "state-owned and privately held", 国有私营) and Huawei, an allegedly private company with close ties to the party state. Even harder to disentangle in terms of party influence and state control mechanisms is a sprawling ecosystem of innovative start-ups, venture capital funds, local and provincial governments and the Chinese military (see exhibit 3).

Exhibit 3

How the party state guides the market

Modes of co-optation of and support for market-orientated companies in the digital economy

Type of influence	Features
Party work	• CCP sets up party committees in companies • Party membership counts as a plus for finding employment • CCP pushes for promotion of crucial projects (like Belt and Road Initiative) • Entrepreneurs co-opted into political institutions
Government support for companies	• Nominating companies to be part of a "national team" • Granting licences to set-up credit-scoring pilot projects • Commissioning digital ID cards project development • Sharing user data to improve algorithms • Setting up incubators and providing tax deductions for tech start-ups • Priviledged access to local, provincial and national procurement markets
Regulations	• Lax or delayed implementation of regulations • Special exemptions
Financing	• Preferred access to capital markets and bank loans • Governments sets up state-backed venture capital funds as investment vehicles • Government buys "special management shares" (1–2 percent of total shares of a listed company)

Source: MERICS

© MERICS

In their push for rapid technological advances, China's leaders are driven by several motives: the need to generate new economic growth through industrial upgrading and boosting innovative business models; the aim of strengthening self-reliance in indigenous innovation and civil-military integration, and the goal of extending China's global influence by expanding the use of Chinese products for digital infrastructures, telecommunications and e-commerce.

Last but not least, China is also driven by the ambition to make governance and control more effective by applying digital technologies for law enforcement.

China's leadership needs to create new, sustainable growth engines to avoid its rise to superpower status being derailed by an economic downturn or social instability. Digitalization is considered crucial for creating a more innovation-driven, competition-based and high-value added economy. The government pursues this goal by pushing for an upgrade of traditional manufacturing industries, by boosting and regulating the digital service sector, and by striving for greater technological self-reliance in high-tech industries.

China is now contending for global leadership in technologies like 5G, quantum computing, AI, or blockchain

China enjoys structural advantages in advancing its bold plans. Beijing channels massive amounts of capital through state guidance funds into emerging technologies and is deterring domestic market entry for foreign competitors to protect domestic companies from competition. Cautious regulatory approaches create leeway for commercial actors to innovate. These advantages have led to substantial growth across multiple sectors, such as logistics, e-commerce, fintech, autonomous driving, and digital health. China is now contending for global leadership in technologies like 5G, AI, quantum computing or blockchain.

However, these structural advantages will not automatically result in Chinese global leadership in all established and emerging technologies. Attempts to overcome dependence in semiconductors have failed.[5] The country continues to struggle with inefficient allocation of funds, and the ongoing tightening of party control over private companies may ultimately hamper innovation.

2.1 DIGITALIZING AND INDUSTRIAL UPGRADING TO MOVE CHINA UP THE VALUE CHAIN

In May 2015, China's government officially announced the Made in China 2025 strategy (MiC 2025), a comprehensive, sector-specific plan for a large-scale digital transformation of China's industry.[6] The implementation and fine-tuning of MiC 2025 are important indicators of the trajectory of China's digital policies. Since its launch four years ago, the strategy is constantly being adapted to a changing environment: In 2017, for instance, the "roadmap" for the strategy was updated and now features core emerging technologies such as 5G, AI and quantum computing more prominently.

Chinese leaders also adjusted self-reliance targets to become even more ambitious, including for the global market share of home-grown technologies (see graphic). These include seabed communication, ultra-low-loss optical fiber production, industrial internet platforms and related security technologies. Domestic demand for global positioning systems (GPS) is to be solely served by China's own Beidou (北斗) system.

China is investing heavily in different areas of technological innovation: For instance, training new talents is a prioritized sphere of action. The "National Talent Development Plan 2010 – 2020" aims to increase the talent pool from 114 million to 180 million by 2020 to support the transition to an innovation-driven growth model. In AI, China intends to establish at least 50 academic and research institutes by 2020.[7] According to calculations, China presently has a pool of around 39,000 AI researchers, less than half than the United States.[8]

Beijing hopes to gain substantial economic benefits by pushing digital innovation within and beyond its borders

China has also announced to invest USD 411 billion between 2020 and 2030 into upgrading its telecommunications systems to 5G. Huawei alone has been investing USD 600 million for R&D in 5G technologies since 2009. The company and its competitor ZTE are rolling out 5G trials across Europe, which is lagging behind China and the US due to regulatory fragmentation and lack of investment.[9]

China has contributed almost two billion USD to the development of ICT infrastructure between 2010 and 2014, outspending traditional donors like UN agencies, EU institutions and Germany. Between 2012 and 2015, Chinese firms participated in merely 7 percent of worldwide undersea cable projects, this ratio is estimated to increase to 20 percent between 2016 and 2019.[10]

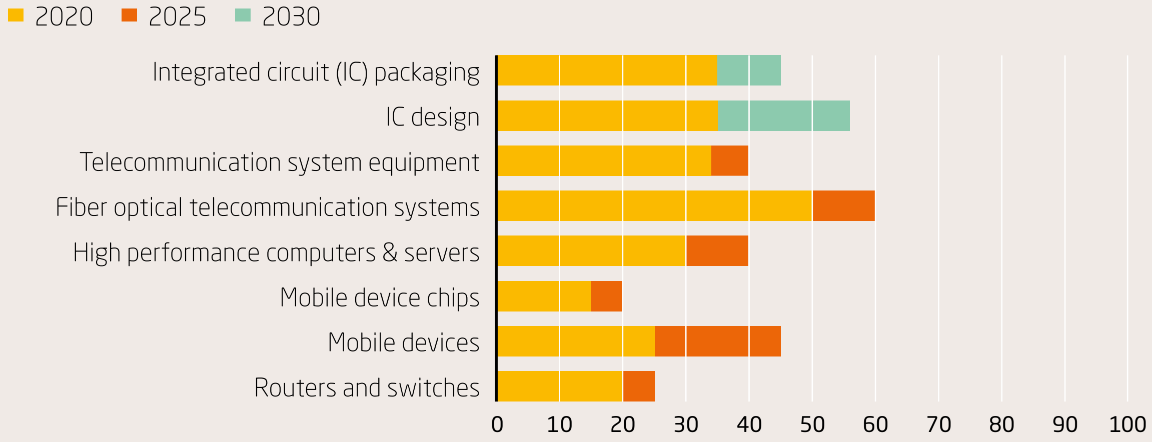
The Chinese government hopes to gain substantial economic benefits by pushing digital innovation within and beyond its borders: for instance, it is estimated that products and developments for the Internet of Things alone could add up to USD 1.8 trillion in cumulative GDP for China by 2030.[11] The size of China's market, state backing, availability of data, and societal openness to the adoption of new technologies, such as mobile payments, have already contributed to a massive growth in Chinese e-commerce, which made up 42 percent of the global market in 2017.[12]

Despite international tensions surrounding China's ambitious plans – it has drawn criticism especially in the United States – European companies and governments (Germany in particular) have been cooperating intensely with Chinese counterparts over recent years and months. In 2018, both Chinese experts and official circles signaled greater openness to foreign participation in the implementation of Made in China 2025, even though this is a contested issue in China domestically: Bodies linked to traditional manufacturing interests like state-owned enterprises (SOEs) and the National Development and Reform Commission (NDRC) tend to opt for self-reliance. Interest groups and actors tied to newly emerging industries seek to benefit more from global innovation dynamics, value chains, and capital flows (see exhibit 4).

Exhibit 4

China is pushing for greater self-reliance in core technologies

Targets for global market share of Chinese IT services and products (in percent)



Source: Technology Roadmap 2015, 2017

© MERICS

2.2 DIGITAL INNOVATION YIELDS QUICK RESULTS AT EXPENSE OF QUALITY AND LABOR CONDITIONS

To incentivize digital innovation, China's government has put several measures in place. For instance, the Internet+ initiative mandated in 2015 is a macro-economic policy campaign to promote the incorporation of the internet, cloud computing, big data and the Internet of Things into a wide range of industries, including agriculture, manufacturing and the service sector.[13] By implementing Internet+, the government also wants to provide jobs to a large and still growing number of graduates who lack employment opportunities. To support this, a campaign on "mass entrepreneurship and innovation" (大众创新万众创业) promotes simplified registration procedures for small businesses and the creation of start-up hubs.

The measures have brought some results, but rapid expansion has come at the expense of quality: The e-commerce sector, for example, has seen double-digit growth, the creation of an immense number of new businesses, apps and services. However, the mushrooming of online shops and delivery services has led to a race to the bottom in prices, product quality, and labor conditions.[14] Likewise, corporate and consumer complaints about intellectual property violations, and the counterfeit and unsafe goods peddled by an army of unregistered small-scale vendors have risen. The Chinese government struggles to find the right balance between incentivizing sector growth on the one hand and controlling the development on the other. A comprehensive law regulating e-commerce came into effect on January 1, 2019. According to foreign experts involved in the drafting process, officials were highly concerned about the independent administrative structures established by some influential companies like online trader Alibaba, which include separate customs arrangements and even security guards.[15]

Beijing still has to find the balance between incentivizing growth and controlling development

The new law puts China partly in line with international standards and other countries' regulations by holding web companies liable for counterfeit and illicit goods sold by third-party vendors on their sites. However, it also formalizes previous de facto protectionist practices common across IT-related industries, banning foreign company from directly engaging in the Chinese market.[16]

2.3 CHINA HAS A LONG WAY TO GO TO ACHIEVE TECHNOLOGICAL SELF-RELIANCE

The existential nature of China's current dependency on foreign-made core technologies is evident to every Chinese leader and increasingly becoming an issue of national debate. Last year, a temporary ban by the United States on exports to the Chinese IT conglomerate ZTE forced the company to halt major business operations.[17] This event, new US export control rules and the ongoing international pushback against telecoms giant Huawei have revived the debate.

In many regards, China still has a way to go to achieve self-reliance in high-tech. For instance, several Chinese semiconductors experts have criticized the nation's existing funding and R&D strategies in the sector as pushing too fast for commercialized outcomes. In the development of Artificial Intelligence technology, China is easily outspending other countries. France, for example, set up an R&D fund of 1.5 billion EUR in April 2018, whereas the Chinese city of Tianjin alone announced a plan to pump 13.5 billion EUR into AI research.[18] China also has a competitive edge in mass data collection and hence the development of algorithms designed for practical, specific tasks.

Some Chinese experts are already warning, however, against creating an “AI bubble” due to government overinvestment and inefficient allocation of funds.

China has, however, made substantial headway in developing the new communications standard 5G. It is the only country that is ahead of the “2020 5G Development Schedule” proposed by the UN’s International Telecommunication Union (ITU). Since 2015, Huawei and ZTE have spent more on 5G than companies in any other country. China has built currently 14.1 network sites per 10,000 people, compared to 4.7 in the United States, and 8.7 in Germany. Only Japan, with 17.4, has built more.[19]

China’s ambition is not only motivated by economic factors: civil-military integration (CMI, 军民融合), a top-level national strategy since 2014, acts as the link between China’s efforts to become a “science and technology superpower” (科技强国) and its plan to build a strong military that can fight and win wars by 2049. It does so by mandating and coordinating greater information and resource sharing between military and civilian institutions. Beijing seeks to leverage private sector high-tech innovation to strive for dominance in emerging dual-use technologies, advance its cyber warfare capabilities, weaponize AI and achieve quantum supremacy.[20]

The Chinese military shares the goal to gain greater control of digital infrastructure, which it needs to strengthen its command and control capabilities: with this objective, it has been laying down undersea fiber-optic cables since the 1990s, including in the South China Sea. The People’s Liberation Army is also set to benefit from the planned extension of the national Beidou Satellite Navigation System’s coverage to over 60 countries along the Belt and Road, a step forward for promoting China’s alternative to US Global Positioning System (GPS).[21]

2.4 SPREADING CHINESE PRODUCTS, SERVICES AND STANDARDS GLOBALLY

The global activities of companies like Huawei, ZTE – and also Alibaba – are in line with a broader strategy promulgated by the Chinese government. Alibaba is moving into Europe[22], promoting its own services, and related regulatory frameworks (the eWTP or e-World Trade Platform) after first implementations in South East Asia and Rwanda.

A regulatory backlash and politicization of IT champions is the biggest challenge to China’s global digital expansion

ZTE and Huawei have managed to become key partners for major telecom operators in advanced economies, including in the EU, deploying the backbone of future global communication networks. China wants to become a major 5G player internationally and Chinese companies are well-positioned in terms of technical capacity. But the ambition meets considerable resistance particularly in the United States, Australia and New Zealand. European countries are also debating whether they want a Chinese company to provide and maintain the 5G networks that will be at the core of innovations in, for instance, autonomous driving, smart manufacturing and other novel applications that need massive online data processing.

A regulatory backlash and politicization of the role of IT champions like Alibaba, Huawei or ZTE in advanced economies and liberal democracies poses the biggest challenge to China’s global digital expansion. This backlash is already underway.

The CCP is eager to support commercial actors in expanding the use of Chinese digital products and services abroad. The “Digital Silk Road” (数字丝绸之路), first aired in 2015 at a roundtable on China-EU digital cooperation, is one integral part of these efforts. The initiative that is sometimes also called “Information Silk Road” (信息丝绸之路) or “Online Silk Road” (网上丝绸之路), serves as an umbrella for a variety of activities whose lowest common denominator is that they are all centered on the idea of enhancing connectivity between China and the world.[23] The Digital BRI covers a range of initiatives revolving around infrastructure, e-commerce, research collaboration, and promoting China’s standards and norms. It has resulted in new major digital infrastructure projects, such as the construction of cable networks connecting Asia and Europe overland jointly undertaken by China and Russia to create an alternative to US-controlled data routes.

China has also made headway in shaping international standards for emerging technologies, securing leadership positions in several international standard setting bodies. In 2015, the CCP leadership established a “Special Leading Small Group on the Major Project of Standardization alongside the ‘Belt and Road Initiative’, 标准联通“一带一路”专项领导小组) to coordinate the efforts. Key priorities include speeding up the promotion of China’s home-grown standards, focusing on “international economic corridors” (Northern China, Mongolia and Russia), and promoting joint research and recognition labs with countries alongside the BRI.[24]

China has secured leadership positions in several international standard setting bodies

After failing to gain majority support in the International Organization for Standardization (ISO) for an alternative Wi-Fi standard in 2011, China today is a leader in the international standardization of blockchain technology, the Internet of Things (IoT) and 5G. In June 2018, China’s IoT Reference Architecture (ISO/IEC 30141), was approved by ISO members. Beijing managed to secure key positions in three main international standard setting bodies, ISO, the International Electrotechnical Commission (IEC) and the International Telecommunications Union (ITU) (see exhibit 5).

Exhibit 5

Setting international standards

Chinese representatives in executive positions of international standardization bodies

	ISO (International Organization for Standardization)	IEC (International Electrotechnical Commission)	ITU (International Telecommunication Union)
Leadership positions	Zhang Xiaogang (President of Ansteel Group Corporation)	Shi Yinbiao, Vice President (President of State Grid Corporation)	Zhao Houlin, ITU Secretary General
Participation in technical committees/ study groups	Secretariats: 64 (of 249) Twinned secretariats:16 Participating members: 685	Secretariat 9 (of 82) Participating members: 182	Chairs: 1 (of 11) Management team positions: 22 Rapporteurs: 51

Source: Websites of ISO, IEC, ITU

© MERICS

China's long-term goal is to change the global landscape of technological competition by defining and exporting their own standards for all emerging industries, thereby ensuring that Chinese products and service are not obstructed by standards set by another country. Chinese experts cite the internet as one major example where US dominance in setting standards severely hampered the development of China's core IT industry and its overall cyber security[25] (see exhibit 6).

Exhibit 6

China's push to shape digitalization on a global scale

The scope of the Digital Silk Road

Type of project	Examples
Developing major infrastructure projects	• Fibre-optic cables across the Arctic Circle • Broadening coverage of Beidou GPS system • Setting up data centers
Promoting Chinese standards	• AI standards (i.e. on algorithmic bias, transparency in algorithmic decision making), 5G, IoT (IoT RA//ISO/IEC 30141, NB-IoT)
Engaging in research collaborations	• Belt and Road Program on Big Earth data collaboration • Partnership between the EU and China on 5G • Technology transfer centers
Raising China's global "discursive power"	• Promoting concepts like "internet sovereignty" • Promoting changes to global internet governance

Source: MERICS

© MERICS

3. Applying digital technology for governance and control

Digitalization is not only considered an economic necessity in China. The ambition goes beyond gaining leadership on global digital marketplaces. China's government wants to use digital technology for effective governance and control over both companies and citizens. Two goals are considered crucial: shielding critical infrastructure and data from foreign access and establishing control mechanisms based on Big Data analysis to monitor economic and societal actors and enforce their compliance.

The CCP leadership's governance approach to cyberspace builds on constantly evolving, inter-related strategies, legal documents and standards. Enforcing cyber security has been a top-priority for the CCP since the arrival of the internet. Maintaining control on different levels is a key driver: cyber security is therefore defined more broadly than in Europe or even in the United States.[26] In China, the term includes not only technological but also ideological and political threats.[27]

3.1 KEEPING FOREIGN FIRMS OUT OF CRITICAL INFRASTRUCTURE AND CONTROL THEIR DATA FLOWS

The Cyber Security Law, in effect since in July 2017, defines key categories like "critical infrastructure" and "personal data" in the widest way possible. The all-encompassing scope of how these terms are defined is the law's most worrying feature.[28] Article 31 contains passages that potentially turn every industry into "critical infrastructure," defining it as:

> *"(…) and other important industries and fields and other key information infrastructure that if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure."*[29]

To further restrict foreign companies' access to China's IT infrastructure, the Cyberspace Administration of China (CAC) is authorized to pursue a cyber security review of all products and services used in critical infrastructures – including exposing the source codes. The CAC has just begun to outline the procedures, and recently published the first list of specified products and services.[30] Source code exposure could become yet another barrier preventing foreign companies from accessing the Chinese market.

Source code exposure could prevent foreign companies from accessing the Chinese market

Network operators are obliged to share information about cyber-attacks, to develop emergency response plans, and be able to quickly address vulnerabilities in their systems. The definition of 'network operators' is vague, though. International legal experts say it can be understood as owners, administrators and service providers, potentially also covering corporates.[31]

Equally worrying are strict requirements on data management for corporates, making them dependent on the good will and further implementation of the authorities involved. Requirements include data localization, meaning companies are forced to store personal information and other "important data" in the PRC.[32] Data localization rules oblige companies to prove that data transfer abroad is necessary, for instance to fulfil contractual obligations. They must perform security assessments before transferring any personal or business data out of China. Companies are also required to obtain user content for using their data, something the authorities currently seem to enforce by regular visits, meetings and monitoring exercises with IT companies. However, detailed guidelines or definitions of the relevant procedures do not exist.

China's regulations are largely modelled on the EU's General Data Protection Rule (GDPR). However, unlike the EU and its member countries, China has so far done little to regulate government use (and abuse) of data. The Cyber Security Law remains a work in progress, with more specific regulations on critical infrastructure and network operators yet to be stipulated. Foreign companies continue to list data security issues among their top concerns.[33] Continued push back from foreign policy makers and companies on the potential scope of the cyber security law's definitions may persuade Beijing to stick with a more flexible enforcement policy for now (see exhibit 7).

Exhibit 7

Europe cares most about data protection

Data protection regimes in comparative perspective

	EU	US	China
Protection of personal data	✓	✓	✓
Constitutional clause on privacy	✓	✓	✓
Availability of judicial mechanism for constitutional protection	✓	✓	✗
Uniform legislation on data protection	✓	✗	✗
Specific data protection authority	✓	✗	✗
Extensive definition of personal information	✓	✗	✓

Source: Shi-Kupfer, Kristin and Chen, George (2018). "Deutsch-Chinesische Plattform Innovation, Policy Briefs 2017 der deutschen Expertengruppe". January 3. http://www.plattform-innovation.de/_media/PolicyBriefs_der_deutschen_Expertengruppe_2017.pdf. Accessed: September 20, 2018

© MERICS

3.2 MONITORING OF CITIZENS' BEHAVIOR

The Chinese government envisions the Social Credit System, a big-data-fuelled mechanism, to become a powerful tool for enforcement of laws, regulations or other party-state targets. Natural persons and legal entities are to be assigned a score, drawing on data from a wide variety of sources. The system is supposed to control adherence to environmental and IPR regulations, but also to more political laws, such as specifications against endangering "national security" or "national unity" (for instance by failing to use the PRC's preferred nomenclature on Taiwan, as happened to international airlines).[34]

The idea is to centralize data on natural persons and legal entities under a single identity (the Unified Social Credit Number), then rate them on the basis of that data, and treat them differently according to their behavior. The system is not yet fully in place and will not be fully completed by 2020, contrary to some media reports. Today, it consists of many separate sub-systems. Once these are linked, however, they may become a powerful instrument to steer citizens and legal entities.

So far, the central government has only implemented the Unified Social Credit Number System and is working on pooling (primarily government) data in a central database. As a nationwide pilot, it has also introduced several blacklist systems. Both individuals and legal entities can be sanctioned for defaulting on debt or, in the case of companies, violating a wide range of laws.

In addition, there are non-mandatory commercial scoring pilots using big data (most importantly Sesame Credit by Alibaba-subsidiary Ant Financial Services, and Tencent Credit), as well as government-run sectoral and local pilots experimenting with behavior ratings of individuals and companies. To have the Social Credit System fully functional one day, the central government depends on manageable data-sets being handed over by private companies. Bureaucracies in China are also reluctant to share data with each other. Private and public players have diverging interests.

The Social Credit System could become an effective tool to shape citizens' and legal entities' behavior

Regulating corporate data protection and storage is therefore a crucial part of the current efforts to get the Social Credit System running. Once these conflicts are resolved, the resulting system could become an effective tool to regulate and shape citizens' and legal entities' behavior, especially if data from China's numerous other surveillance projects, such as those currently tested in Xinjiang (see below) are all tied together.

3.3 CENSORING INTERNET AND CYBERSPACE

Alongside an expanding grip on data, the CCP has also consistently tightened regulations on internet content to ensure officially acceptable views remain the dominant voice in Chinese cyberspace. Since 2017, the government has reached into more channels of communication, closing in on 'hidden spaces' for pluralistic exchange of information and opinion. For example, in September 2017, the CAC made chat group providers, as well as administrators of private groups, liable for the content of discussions, required them to store user data for six months, and apply a credit scoring system to the services they offer.[35]

The basis for China's censorship regime is the so-called Great Firewall, which uses various sophisticated tools to block and filter internet traffic.[37] The government also continues to foster self-censorship through the arbitrary prohibition of widely-defined 'illegal content,' with users as well as IT companies. The leadership has also started to issue more explicit legislation to make previously often laxly enforced requirements like the real-name registration system more effective.

The restive region of Xinjiang currently serves as a worrying example where China's quest for societal control may lead to: Huge amounts of data are currently being collected in the northwestern Autonomous Region. There, Beijing has established an IT-based surveillance state in the name of security measures against terrorists. By trying to contain the Uighur muslim community, the Chinese authorities have also created a testing ground for AI applications: Algorithms, e.g. for facial recognition tools, can be enhanced by feeding them the large amounts of data gathered in video and other surveillance measures.

Case Study 1: 5G

CHINA'S LEADERSHIP IN 5G FACES A GLOBAL BACKLASH

Global competition surrounds the development of the powerful telecommunications standard 5G: US providers had secured their leadership on the preceding systems, 3G and 4G. China is determined to win the ongoing race to install next generation networks across the globe.

Activities and motives: Scale-up and standardize

China considers leadership in 5G and related technologies such as autonomous driving, industrial automation and smart cities as critically important for both security and economic reasons.[36] The "Made in China 2025" strategy documents issued in 2015 gave prominent mentions to 5G, aiming for a "comprehensive breakthrough of 5G technology". Likewise, the 13th Five-Year Plan (2016 – 2020) called 5G a "key emerging industry" and suggested a 2020 launch date.

China's leadership in 5G benefits from intense national coordination in the telecoms industry. All three mobile network carriers have committed to meet the government's timeline. Two of them (China Unicom and China Telecom) have even started initial negotiations on a state-controlled merger that might further accelerate 5G expansion. Mobile carriers have already conducted 5G tests in major urban centers (Beijing, Shanghai, and Shenzhen) and are poised for a partial commercial launch by 2019. State-owned companies have pushed ahead to develop 5G standards jointly with the government and to introduce them to international standardization bodies.

Achievements: Ready for commercialization, ahead of UN schedule

China has outspent everyone else in its ambition to advance 5G, most notably the second contender, the United States (by 24 billion USD since 2015). China's MIIT announced plans to invest an additional 411 billion USD up to 2030, with peak spend in 2023. China will soon host the largest 5G trial area in the Yangtse-Delta. Since 2015, Huawei and others, have spent more on 5G than companies in any other country, e.g., by building infrastructure. China currently has 14.1 network sites per 10,000 people, compared to 4.7 in the US and 8.7 in Germany; only Japan, with 17.4, has built more. In 2017, China Tower added more sites in three months (460 sites per day) then US tower companies and carriers did in the last three years.[37]

As well as having a first mover advantage, China can also count on high domestic demand, which will enable the country to roll out the new digital highways faster than anyone else. It has the worlds' largest mobile phone user market – three times the size of the US. Sector-watchers expect the number of 5G users in China will reach 576 million by 2025, equivalent to 40 percent of global consumption.[38]

China also will benefit from a technological advantage: it will be able to pursue a non-standalone 5G roll-out by making use of existing 4G/LTE-networks. 5G will run on a similar wavelength spectrum to the one that is currently used. In the US, the same frequencies are already largely occupied. Providers have to focus on the harder-to-control high frequencies and build new infrastructure. China will also need to make use of the higher frequencies eventually to exploit the maximum bandwith of 5G but at present it is under less pressure than other countries.

China is the only country that is ahead of the UN's International Telecommunication Union (ITU)' 2020 5G development schedule. It also has taken the lead role in 3GPP, the 5G group of the International Standardization Organization (ISO), submitting 40 percent of the standards and 32 percent of the documents.[39]

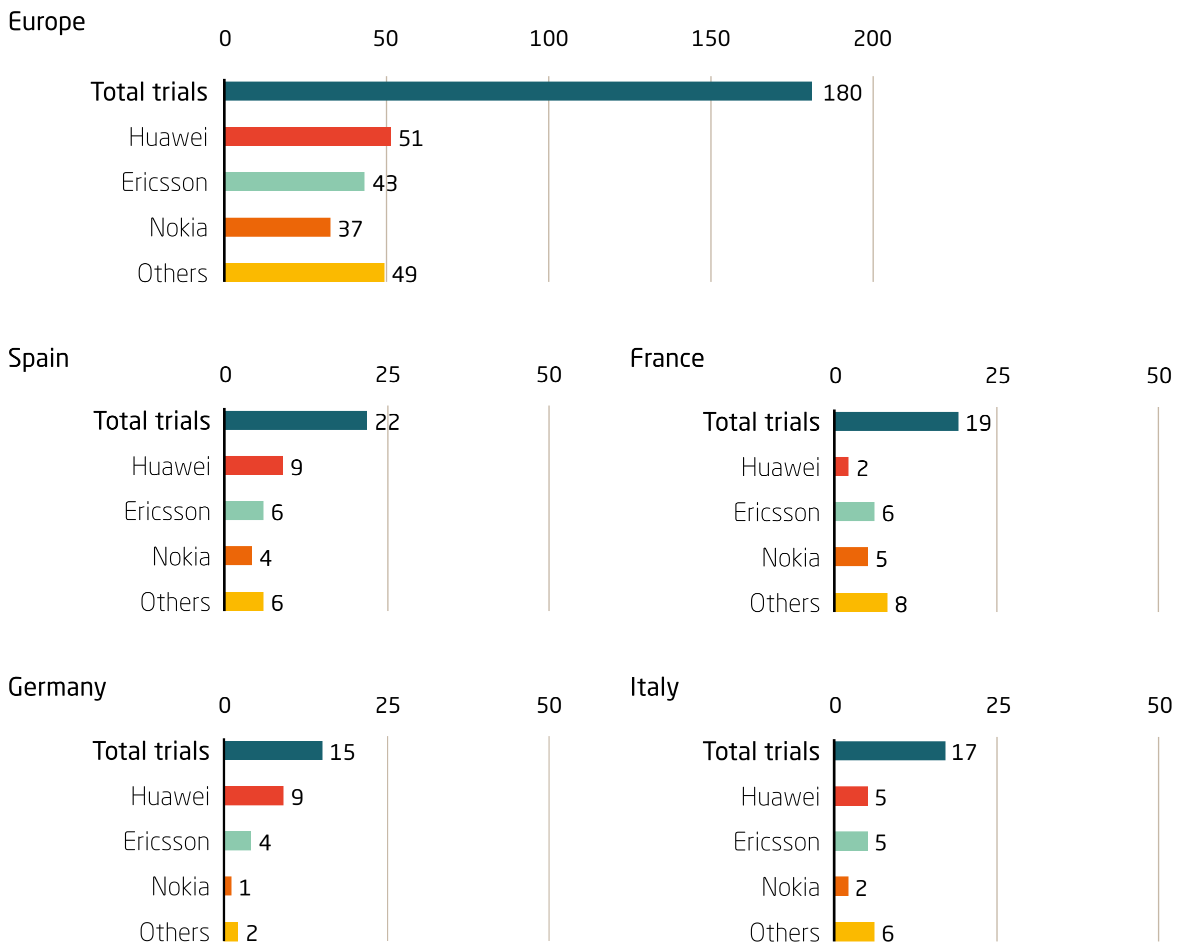
Challenges: International backlash

Currently, the biggest risk to China's global leadership on 5G is the international backlash against Chinese companies as providers of critical infrastructure. Huawei and ZTE have already been banned from selling their equipment to the US, Australia and New Zealand. Other governments are likely to follow the coordinated advice by the "5 Eyes" (US, UK, AUS, NZ, CAN) network of intelligence services. This might lead to a bifurcated 5G world, where some countries would use Huawei's 5G standard and others different, non-compatible standards.

Exhibit 8

Huawei is the main manufacturer of 5G trial equipment in Europe

5G trials in Europe and the four most active countries by hardware manufacturer



Source: 5G-Observatory. https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/. Accessed: March 14, 2019.

© MERICS

Case Study 2: Artificial Intelligence

CHINA IS TORN BETWEEN COOPERATION AND SELF-RELIANCE IN AI

In 2016, the AlphaGo program developed by Google's DeepMind defeated Lee Sedoul, the Korean world champion Go player, at the strategic board game. It was a sputnik moment for China's policy makers, who became determined to catch up with US firms in AI research and development.

Activities and motives: Scaling up and leveraging cooperation

In July 2017, China's government published a comprehensive AI development plan that clearly stated China's ambition to become "the global leader in AI fundamental theory, standardization, technological development and application by 2030."[40] It was a switch in tone from the more gradual targets in previous industrial policy blueprints such as "Made in China 2025." There, Beijing had pointed out the importance of developing AI open-source software and highlighting how cross-border and collaborative efforts had shaped the field.

"Made in China 2025" called on domestic companies to build an industry worth more than 150 billion USD, supporting the target with huge funding announcements. Where France's President Macron set up a national R&D fund of 1.5 billion EUR, China pledged AI funding of 13.5 billion EUR to a single city, Tianjin.[41]

Achievements: Quantitative leadership

China's central government funds the core AI-related research projects of big players like Alibaba, Baidu and Tencent. It has also invested heavily in leading start-ups like Cambricon Technologies, which specializes in AI development and chips.

On purely quantitative indicators, China seems well on track to achieve its global AI leadership goals. China tops most quantitative rankings, e.g., scale of global funding attracted; number of patents; scale of R&D investment.[42] For example, China filed 30,000 patents in 2018, or2.5 times more than the US, which it surpassed in 2015.[43]

However, quantitative assessments have limitations, as shown by debate on the decreasing usefulness of data *volume per se* – one of China's often-cited core advantages.

Challenges: Dependency on foreign suppliers

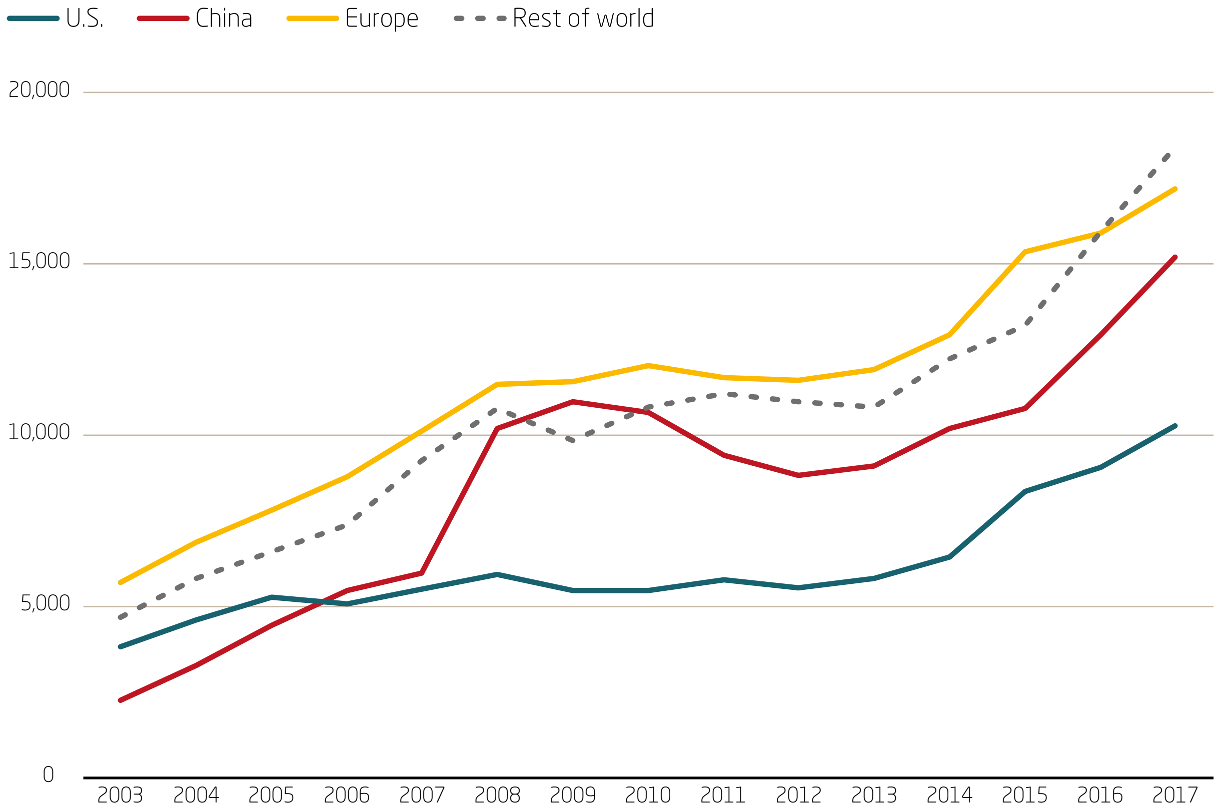
China's key challenges in AI are very similar to those it faces in other core high tech industries: its dependence on foreign suppliers of chips and a critical lack of skilled talent. China's experts have also warned against creating an "AI bubble" through government overinvestment and inefficient allocation of funds.[44]

China's leadership knows it needs to balance ambitious leadership with vital international cooperation to maintain progress in AI development. Global AI investment is highly entangled and cross-border: Spin-off firms of Baidu, Alibaba and Tencent have set up research centres in Silicon Valley and are increasingly moving R&D into Europe. At the same time, China is becoming a global exporter of AI surveillance technologies and reaching out into other markets with customized products and services.[45]

Exhibit 9

China's AI research is rapidly catching up

Annually published AI papers by Elsevier, by region (2003 – 2017)



Source: Shoham, Yoav et al. (2019). "Artificial Intelligence Index 2018 - Annual Report". AI Index. http://cdn.aiindex.org/2018/AI Index 2018 Annual Report.pdf. Accessed: March 13, 2019.

© MERICS

Case Study 3: Blockchain

CHINA STRUGGLES TO BALANCE DECENTRALIZED NETWORK SECURITY WITH CENTRAL CONTROL

China takes a unique approach to blockchain technology, eager to exploit its potential and yet, at the same time, to centralize control over this genuinely decentralized technology. China's Cyberspace Administration (CAC) published new regulations in February 2019 requiring all blockchain companies to register their users and to hand personal data and activity sheets over to the authority on request. The PRC banned international crypto-currencies in 2017 because of their potential to destabilize the financial system. Raising funds for new cryptocurrency projects is prohibited,[46] and a committee has been tasked with detecting fraudulent blockchains.

Activities and motives: Harnessing private sector innovation

President Xi Jinping called blockchain "a breakthrough technology" in May 2018; a month later a CCTV2 documentary described blockchain as 10 times more valuable than the internet. There is a blockchain educational guide for officials, and the People's Bank of China (PBoC) has published several white papers on blockchain.

Chinese private investors and companies practically ran the Bitcoin business by themselves until a clampdown in 2017. Between 2010 and 2018, average funding for blockchain projects was higher in China than anywhere else (25 million USD)[47]. Today, the private sector is being increasingly replaced by local governments. Authorities in the eight biggest blockchain hubs have set aside 3.57 billion USD for project development since 2016.[48]

Achievements: Catching up and expanding the spectrum of applications

The race for technological leadership in blockchain technology is a close one: the United States outstrips all other countries in the number of startups and total funding of blockchain companies. However, a recent survey of international tech executives found most respondents saw China as the emerging blockchain leader.[49] China ranks third in total blockchain-related spending by region.[50] Chinese companies filed more than half of blockchain patents worldwide in 2017 (225 out of 406).

Many applications are being pioneered in China: Chancheng district civil administration with 1.3 million residents in Guangdong Province has been lifted onto a blockchain. A recent addition was the so-called community correction application (区块链+社区矫正), which tracks and evaluates the movement of former prison inmates. Since September 2018, China's Supreme Court has accepted evidence in legal disputes on blockchain. Perhaps the most notable project is the PBOC's ongoing attempt to develop crypto RMB in order to establish a "cashless society".

China's large numbers of blockchain personnel is likely its greatest strength. Although some people left after international crypto-currencies were banned, the majority stayed and now form a workforce of highly specialized engineers. Organizations in China are hiring more staff with blockchain experience[51] than anywhere else.

Challenges: Finding a suitable level of political control

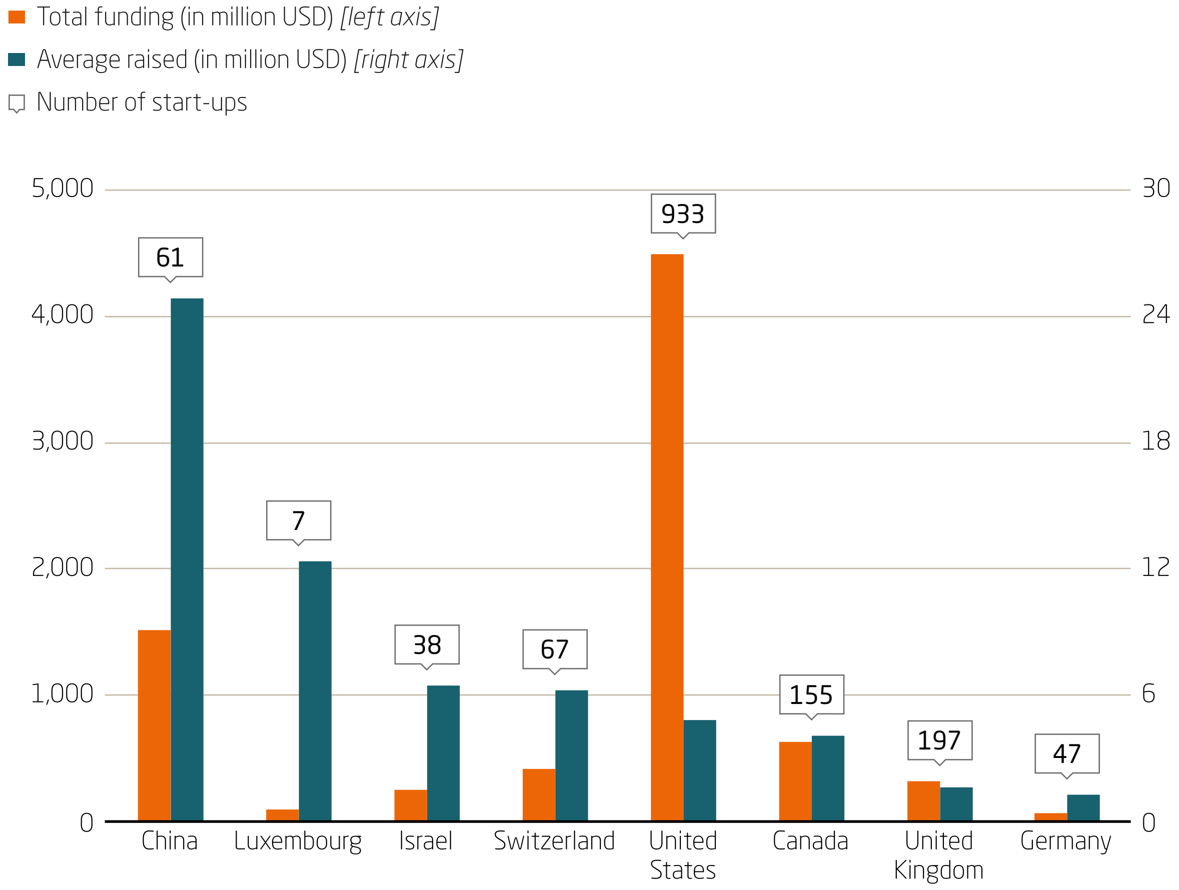
The biggest obstacle to the establishment of blockchain technologies over a wide range of sectors is the CCP's uncertainty: Its policies veer between protectionist measures and development stimuli. Companies are hesitant to develop successful applications further and are waiting for policy normalization.[52] Interaction with international tech circles has become more difficult since international blockchains were banned in China. Domestic specialists must therefore become self-reliant to find solutions. The current approach of exerting central control over blockchains (which are decentralized by inherent design) could lead to interoperability issues and less robust algorithms.

Isolation makes future conflicts over blockchain standards almost inevitable. Some challenges are already visible on the horizon: the data that blockchain companies must register with the CAC can potentially be scrutinized by China's authorities at any time. Governments and citizens of other countries interacting with Chinese blockchains may soon face a similar dilemma as in the 5G question and will have to decide whether to sacrifice data security for economic benefits. Some observers believe that a blockchain with Chinese characteristics similar to the self-enclosed Chinese internet, is already in the making.

Exhibit 10

Chinese start-ups receive most funding,the US spends three times most in total

Sorted by average funding per start-up



Source: Wen, Fan (2018). Blockchain Start-ups (2000-2018). https://public.tableau.com/profile/fan.wen5373#!/vizhome/Blockchain_Companies/MapofStartups. Accessed: March 20, 2019

Case Study 4: Quantum computing

CHINA IS STRIVING FOR QUANTUM HEGEMONY

China achieved a major breakthrough in quantum communications when researchers conducted the first quantum video call between Beijing and Vienna in September 2017. Encrypted information was embedded in photons (particles of light) in a hybrid quantum state. Quantum communication is thought to be unhackable. Attempts to eavesdrop on data packets would lead to a collapse of the photon's quantum state and be immediately obvious.[53]

Activities and motives: Quantum supremacy and military usability

Since 2015, the CCP has accelerated its quest for leadership in quantum technology, a fast-moving field of research. Quantum computing, communications and sensoring were included in the "Made in China 2025" strategy, and in the 13th Five-Year-Plan (2016 – 2020). The Civil-Military Fusion Plan (2017) also mentions the technology prominently.

China has spent at least ten times more on quantum R&D than the United States, with estimates starting from 50 billion USD.[54] China overtook the US in patent numbers, in 2016 and filed twice as many in 2017 . China is the leading source of new inventions in quantum encryption, ranks second in quantum sensoring, and fifth in quantum computing-related filings.[55]

The central government is providing more than 220 million EUR for quantum research and development. Several local centers and provincial initiatives are also emerging. For example, the province of Anhui set up a fund of nearly 1.6 billion USD in 2017 and intends to build the world's biggest quantum research facility. Work there will help China achieve "quantum supremacy" by 2020, according to China's leading quantum scientist, Pan Jianwei.

The potential military usability of quantum technologies is an important motive for China's investment[56]: funding is coming from the PLA itself, notably the recently created Strategic Support Forces, as well as state-owned defense conglomerates in the shipping and aviation sectors partnered with academic institutions.[57]

Achievements: Pioneering tests for new applications

China has pioneered tests of new applications, successful solution to problems (i.e. night time communication) and broken several world records for the scope of quantum entanglement and launched the world's first quantum chip-based cloud computing platform. Unlike other emerging technologies, China is self-reliant in necessary components like quantum repeaters or quantum chips.[58]

Challenges: Tech-nationalistic megaprojects

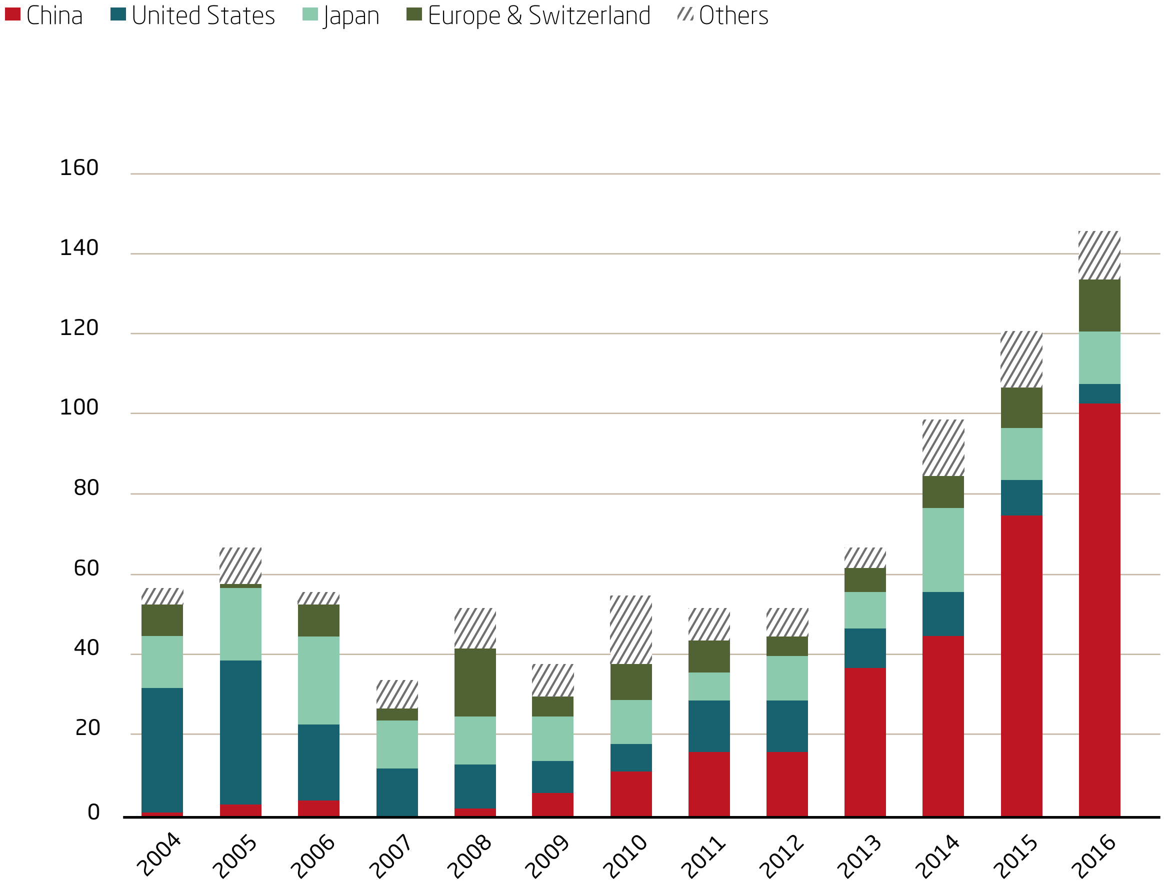
It is hard to evaluate the maturity of projects in quantum radar or navigation, partly because military research lacks transparency. China's researchers have voiced concern over the government's exaggerated emphasis on military applications, the likely inefficiency of excessive spending, and overly-narrow focus on tech-nationalistic "largest and fastest" megaprojects.

Looking ahead, a key factor to watch will be whether China can succeed in further developing and operationalizing military applications, such as quantum radar to detect stealth fighters. Another is whether, and when, China is able to expand its quantum communications network to become fully operational.[59] So far, China's breakthrough projects have been based on close cooperation with foreign researchers, mostly in Europe. The overall political atmosphere may influence whether and how far these collaborations can be continued.

Exhibit 11

China's quantum efforts are all about encryption

China's patent filing related to quantum encryption according to the European Patent Office Global Patent Index



Source: Travagnin, Martino (2019). "Patent analysis of selected quantum technologies". Joint Research Centre, European Commission. https://ec.europa.eu/jrc/en/publication/patent-analysis-selected-quantum-technologies. Accessed: March 30, 2019.

© MERICS

4. China's digital offensive brings more security risks than cooperation opportunities for Europe

China's encompassing and ambitious digital policies contrast with the EU's still fragmented strategy. Today, China's digital transformation is already impacting Europe in at least three different ways: it raises issues related to (fair) economic competition, it creates uncertainties and direct security risks related to cybercrime and critical infrastructures, and it is likely to challenge EU norms for human security and privacy protection.

At the same time, China's digital offensive offers technological and financial alternatives to the dominant US-provided digital solutions and business models. There will be implications for navigating EU-China relations, and for the transatlantic alliance, as European actors explore room for cooperation whilst pre-empting security risks in an increasingly high-stakes game.

4.1 EUROPE NEEDS TO MANAGE ECONOMIC COMPETITION, ENTANGLEMENT AND DEPENDENCY

In some areas, complementary technological strengths and weaknesses create co-operation incentives at the political and the industrial levels. For instance, China's strength in business models and integrated applications complements the European technological lead in smart manufacturing and the Internet of Things. However, the expansion of Chinese companies into European markets will deepen existing concerns over technology transfer and throw up fresh challenges, especially how to manage greater entanglement in the Chinese digital market. The agenda of pressing new issues is likely to include fair competition rules for investment, IP protection in research collaborations and how to manage and regulate cross-border e-commerce and data-flows between the EU and China.

Chinese IT companies are already reaching deep into critical European digital infrastructures

The growing presence of Chinese ICT companies is shaking up digital markets in Europe. Chinese e-commerce giants such as Alibaba or JD.com not only challenge European competitors with new business models. Their involvement raises challenges for the regulatory framework of the European Digital Single Market. At the same time, Chinese IT companies like Huawei or Dahua Technologies are already reaching deep into critical European digital infrastructures. Given the lack of price-competitive European (or US) alternatives, many European member states are vulnerable to dependency, lock-in effects and security risks.

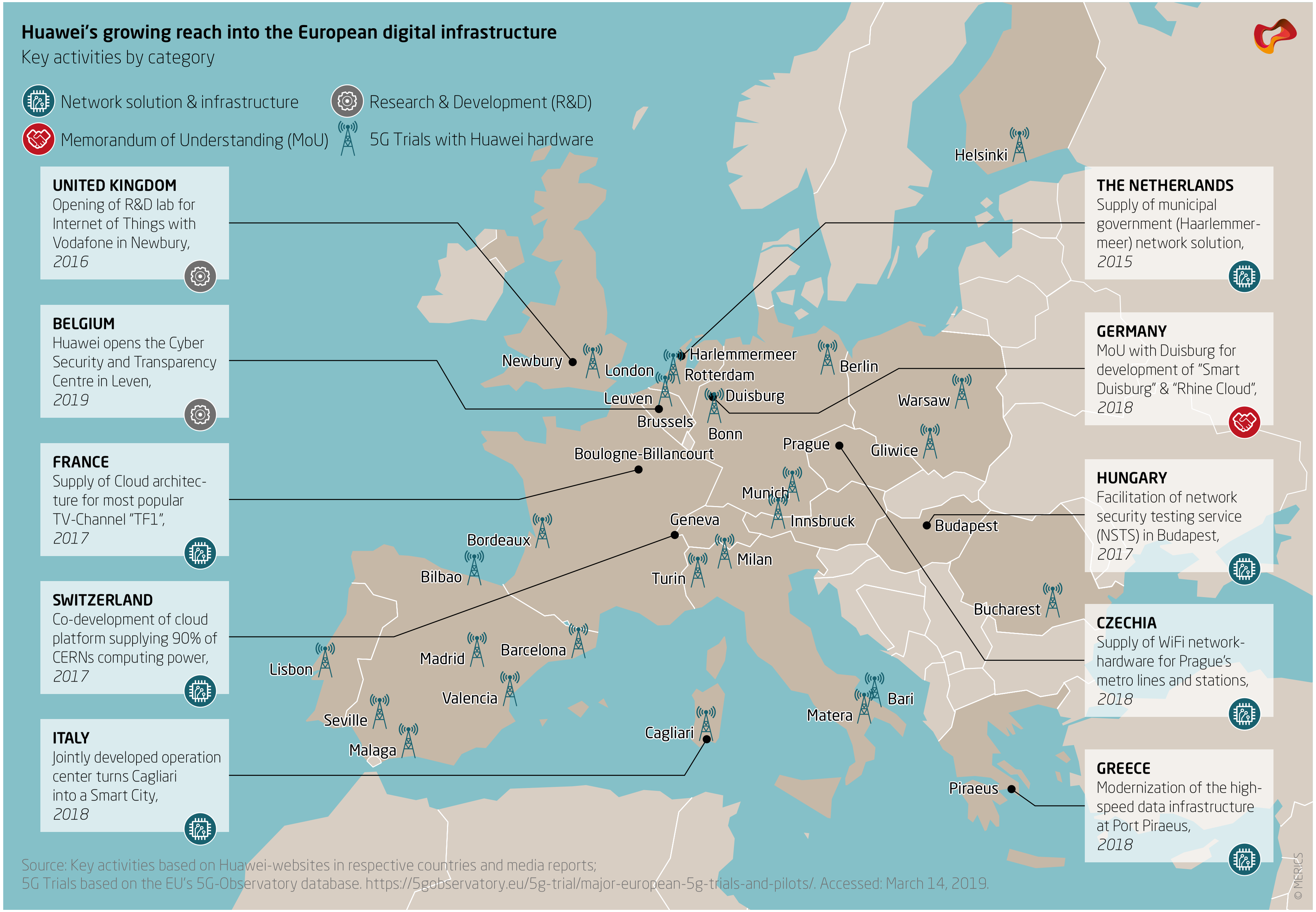
Chinese e-commerce, finance, logistics and data companies could play a positive role in connecting the European continent, provide European customers with attractive products and services, and potentially serve as alternatives to dominant US solutions. However, the issue of fair competition needs to be tackled urgently, given that all Chinese digital tech leaders continue to benefit massively from protectionism at home or other means of government support.

Likewise, Chinese companies also offer unique opportunities for R&D collaboration increasingly at the leading edge of technological developments. By 2018, Huawei had set up at least 23 R&D centers across Europe, doing work on 5G, IoT, and chips. Midea and Haier both have R&D research labs focusing on developing smart home appliances in Europe.[60]

Exhibit 12

Huawei's growing reach into the European digital infrastructure

Key activities by category



UNITED KINGDOM
Opening of R&D lab for Internet of Things with Vodafone in Newbury,
2016

BELGIUM
Huawei opens the Cyber Security and Transparency Centre in Leven,
2019

FRANCE
Supply of Cloud architecture for most popular TV-Channel "TF1",
2017

SWITZERLAND
Co-development of cloud platform supplying 90% of CERNs computing power,
2017

ITALY
Jointly developed operation center turns Cagliari into a Smart City,
2018

THE NETHERLANDS
Supply of municipal government (Haarlemmermeer) network solution,
2015

GERMANY
MoU with Duisburg for development of "Smart Duisburg" & "Rhine Cloud",
2018

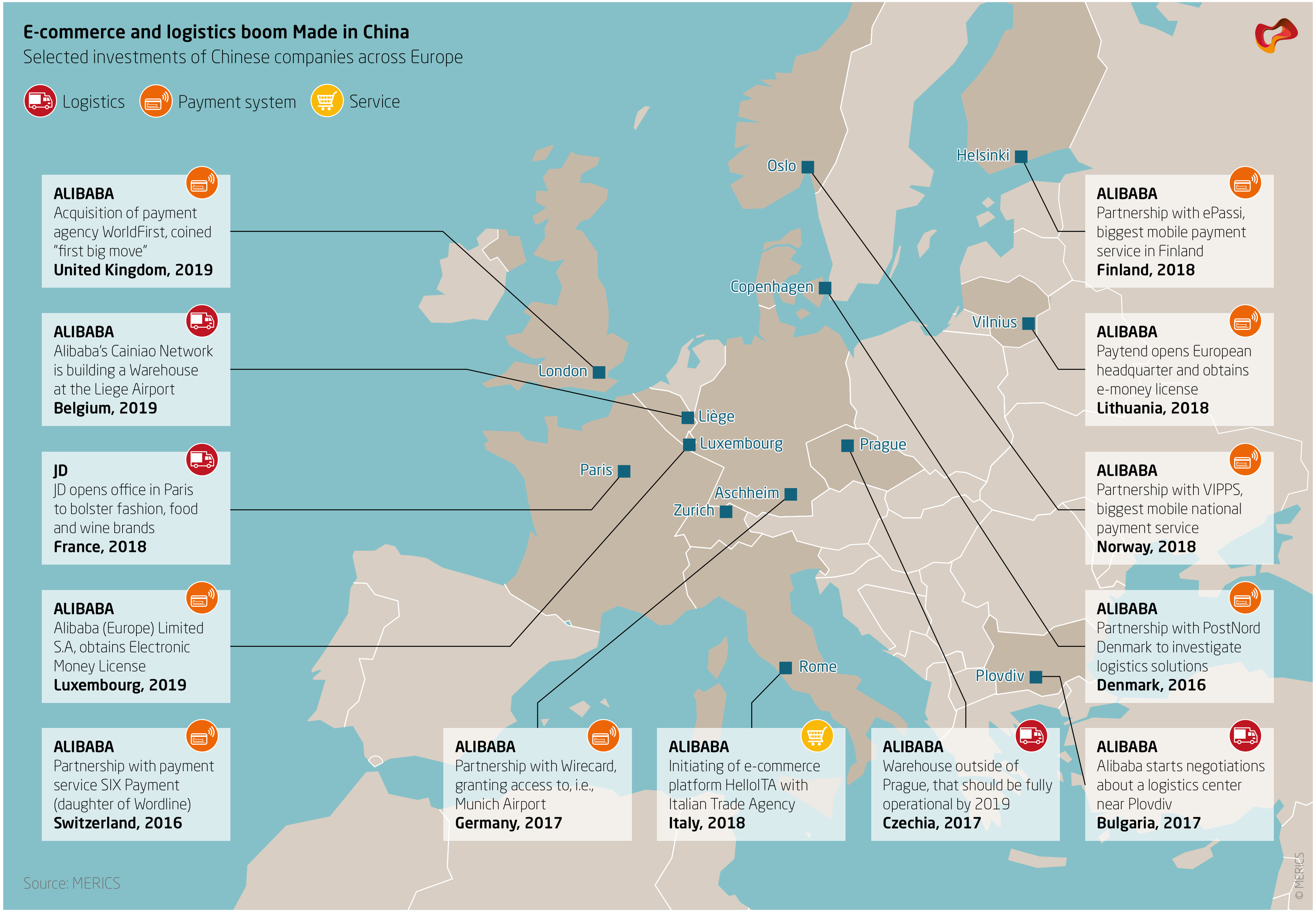
HUNGARY
Facilitation of network security testing service (NSTS) in Budapest,
2017

CZECHIA
Supply of WiFi network-hardware for Prague's metro lines and stations,
2018

GREECE
Modernization of the high-speed data infrastructure at Port Piraeus,
2018

Source: Key activities based on Huawei-websites in respective countries and media reports;
5G Trials based on the EU's 5G-Observatory database. https://5gobservatory.eu/5g-trial/major-european-5g-trials-and-pilots/. Accessed: March 14, 2019.

Exhibit 13



E-commerce and logistics boom Made in China

Selected investments of Chinese companies across Europe

ALIBABA
Acquisition of payment agency WorldFirst, coined "first big move"
United Kingdom, 2019

ALIBABA
Alibaba's Cainiao Network is building a Warehouse at the Liege Airport
Belgium, 2019

JD
JD opens office in Paris to bolster fashion, food and wine brands
France, 2018

ALIBABA
Alibaba (Europe) Limited S.A, obtains Electronic Money License
Luxembourg, 2019

ALIBABA
Partnership with payment service SIX Payment (daughter of Wordline)
Switzerland, 2016

ALIBABA
Partnership with Wirecard, granting access to, i.e., Munich Airport
Germany, 2017

ALIBABA
Initiating of e-commerce platform HelloITA with Italian Trade Agency
Italy, 2018

ALIBABA
Warehouse outside of Prague, that should be fully operational by 2019
Czechia, 2017

ALIBABA
Alibaba starts negotiations about a logistics center near Plovdiv
Bulgaria, 2017

ALIBABA
Partnership with ePassi, biggest mobile payment service in Finland
Finland, 2018

ALIBABA
Paytend opens European headquarter and obtains e-money license
Lithuania, 2018

ALIBABA
Partnership with VIPPS, biggest mobile national payment service
Norway, 2018

ALIBABA
Partnership with PostNord Denmark to investigate logistics solutions
Denmark, 2016

Source: MERICS

However, China's quest to attract leading researchers may turn joint research projects into channels of IP loss and EU brain drain. Attracting and keeping the best scientific brains is a persistent area of concern for the EU.[61] China has long relied on sending students overseas to the world's leading institutes and reaping the benefits when they return with capabilities and networks.[62]

The latest investment announcement by Alibaba to create a smart logistics hub in Liege, Belgium, highlights potential new challenges that Chinese digital giants will create for Europe.[63] As such activities are endorsed and potentially also subsidized by the Chinese state, Chinese digital services establish distorted pricing schemes in terms of costs of services.

Moreover, the Alibaba-led, but government supported global initiative for cross-border e-commerce, Electronic World Trade Platform (eWTP) should be scrutinized for its potential to undermine a Digital Single Market on European terms and with regard to the security of data flows and storage. By making European governments subscribe to eWTP, China might grant them limited access to an otherwise still restricted digital market in the PRC while Chinese firms can profit from Europe's openness and EU standardization (see exhibits 12 and 13).

4.2 EUROPE NEEDS TO PROACTIVELY ASSESS RISKS OF CHINESE IT ACTIVITIES FOR CRITICAL INFRASTRUCTURE

Chinese IT companies have long extended their reach into Europe's digital infrastructure, featuring prominently in critical infrastructure, like 3G and 4G mobile networks. However, it was only in 2018 and 2019 that Huawei's engagement in building up European mobile networks came under wider scrutiny. Hence, the auctioning of 5G network frequencies in EU member states was accompanied by stark warnings about Huawei's credentials by several European intelligence agencies and outright bans by allies and like-minded countries.

Huawei would find it hard to refuse to help with intelligence gathering if requested by Beijing

The unease of intelligence agencies seems to be driven less by "smoking guns" and more by technological "known unknowns" and the difficulty in detecting illegitimate data flows in a timely manner and/or ruling them out reliably. Another major concern has been related to the question whether or not Huawei would be legally forced to cooperate with the Chinese government, i.e. handing over data, in the name of "national security".

Citing work commissioned to international law firms, Huawei has kept pointing out that the company is not obliged by law to cooperate with the Chinese government in their national intelligence work. Many experts, however, argue that Huawei would find it hard to refuse to help with intelligence gathering in its overseas business if requested by Beijing, and crucially based on China's National Security Law.[64] The compulsory co-operation clauses in China's National Intelligence Law suggests that Chinese companies could be pressured to collect and hand over data to China's government beyond what is permitted within the European legal framework.

While most European governments have shied away from debating the merits and pitfalls of an outright ban on Huawei, the British network operator BT decided in December 2018 to block the Chinese IT enterprise from providing 5G solutions, and it also decided to remove Huawei equipment from previous generations of telecommunication standards. Similarly, Vodafone put in place a temporary ban for Huawei hardware in core networks.

However, with Huawei still likely to feature in many European 5G networks, the risk of governments has shifted into the realm of security risk mitigation. Theoretically, technical security risks could be mitigated through ambitious screening mechanisms of Huawei's (or other relevant company's) hardware and code, but these would need to be deployed across Europe and have, where existent for longer periods of time, like in the UK, failed to generate the necessary trust. Hence, leading British security officials had made the rare move of raising security concerns publicly, after the annual report by the Huawei Cyber Security Evaluation Center Oversight Board in Summer 2018 raised doubts for the first time about specific security guarantees provided by Huawei.[65]

Analysts have suggested that the discussion around Huawei's role in creating Europe's 5G infrastructure came too late and that a more consistent regulatory and security approach could have been developed across Europe, if EU member states and Brussels had engaged in a coordinated and proactive risk assessment approach at an earlier stage. Indeed, in moving forward, the discussions surrounding the rollout of 5G networks will prove to be nothing but the tip of the iceberg. In the coming years, European countries will be forced to permanently evaluate the opportunities and risks associated with cooperating with Chinese companies in the rollout of new tech developments. Chinese tech giants, like ZTE or Huawei, supply a full range of digital services – from fiber cable and network services, routers or mobile phones, to cloud-based storage and software solutions for IoT devices like video cameras across Europe.

A case in point when it comes to a "bundled rollout" of many of these technologies and the need to devise a proactive European response is the global expansion of the "smart cities" concept, of which Huawei is a main proponent. Such smart cities revolve around cloud computing and "Internet of Things" technologies in urban management tasks like resource optimization and public services allocation, ranging from policing, traffic management, to waste management to environmental protection measures. China is a leader in trialling smart cities, so it is natural that Chinese companies are extending their global reach in this field. According to consulting firm Deloitte, China had about 500 smart city projects in 2018, or half of the global total of 1,000 projects.[66]

EU governments have asked very few questions about risks associated with China's tech giants supporting smart city development

In Europe, it is likely that smart city projects will initially consist of a range of individual projects that improve government services – from traffic management to environmental protection.[67] However, there is a major difference in what Europe seeks to get out of smart city projects and what Chinese companies might seek to deliver. In China, smart cities support a larger process that the CCP terms 'social management'[68], a process directly aimed at improving the party-state's governance capacity. They fit within the CCP's efforts to integrate[69] political control within the same systems that contribute to China's economic and social development. China's approach to smart cities includes improved public services, but also massively enhances the potential for state surveillance, even if it is currently less sophisticated[70] than some reports suggest.[71] In the past few years, this effort has been particularly visible in regions like Xinjiang and Tibet.[72]

Nonetheless, European governments have asked very few questions about the long-term risks associated with allowing China's tech giants to support smart city development. Huawei is one of the key Chinese companies involved in early European smart cities agreements and has signed several MOUs across Europe:

- Duisburg, Germany: Huawei and the German city of Duisburg have signed a Memorandum of Understanding for an all-encompassing smart city plan. The "Rhine Cloud Framework Agreement" proposes integrating "e-Government, transportation, IoT and unified communication", or "'Smart Duisburg 1.0"'. A second phase envisions the development of Smart Duisburg 2.0, including 5G and Wi-Fi.[73]
- Malta: Huawei has signed an MOU, including areas like public safety, video analytics, data processing and IT systems.[74]
- Sardinia, Italy: Huawei provides an eLTE broadband solution that includes video surveillance, weather and environmental sensors. Huawei has also opened a joint innovation center on the island.[75]
- Belgrade, Serbia: Huawei has signed a Strategic Partnership Agreement with the Ministry of the Interior and has begun implementing the first phase with deployment of video surveillance and intelligent analysis systems.[76]

Apart from smart cities, Central and Eastern Europe have recently become popular entry points into the European market. By entering into a co-operation with a local partner, multi-service providers like Alibaba, Huawei and more specialist companies like video surveillance solutions provider Dahua are seeking to expand their business further into Western Europe.[77]

4.3 EUROPE NEEDS TO MITIGATE CYBER SECURITY RISKS

The 2013 EU Cyber security strategy identifies potential physical vulnerabilities connected to security risks from intentional or accidental failure of IoT systems, and to cyber-crime activities like economic espionage or political manipulation.[78] China's digital reach into Europe is a potential concern for all of those areas: some effects have already taken shape.

The Internet of Things is a sector in which low-quality connected devices from China might pose a security risk. IoT is a rapidly expanding market, whose value is likely to reach USD 163 billion in 2020. Forecasts suggest that 95 percent of roughly 200 billion connected devices globally will be made in the PRC by 2020.[79] Given the lack of nationwide standards for IoT devices, cheap and low-quality products from China pose a security risk to Europe, as has been shown in the past.

Forecasts suggest that 95 percent of roughly 200 billion connected devices globally will be made in the PRC by 2020

The spread of unsecured Chinese devices is thought to have contributed to a massive increase in Distributed denial of service attacks (DDOS) in Europe.[80]

A case dating back to October 2017 highlights the risks of injecting faulty products into the market: At the time, IoT device manufacturer Xiongmai Technology issued a partial recall of its products in response to a DDoS attack, when millions of households and home security systems infected by Mirai malware acted as "attackers.", Xiongmai recalled electronics boards for digital video recorders and IP cameras and offered security patches. However, the company later denied responsibility, blaming users for not setting individual passwords for the devices that were not password-protected by default. Recent research found that Xiongmai still has not followed up on warnings by security experts and never provided the necessary patches.

The EU and China have set up a cooperation network on IoT issues. However, it is currently focused on high-end services and large-scale projects such as smart agriculture, smart cities or autonomous driving.[81] To counter security risks from low-tech IoT in household use, the current Sino-EU cooperation on standardization, involving industrial production and safety checks, would need to be expanded.

Cybercrime and espionage from China are increasingly worrying risks Europe has to face

Cybercrime and espionage from China are two increasingly worrying risks Europe has to face.[82] Companies are disinclined to report cyber incidents, but according to security insiders the corporate sector is a key target for Chinese espionage. The EU has not set up a formal government-to-government Cyber Security Dialogue with China. Instead, there is a broad framework including a task force and a Track 1.5 dialogue. The US does have a formal, bilateral dialogue and, at one point, reached an agreement to prevent cyberattacks originating from state agencies and departments. Experts increasingly agree that the result was merely a temporary decline in hacking and espionage activities by Chinese entities.[83]

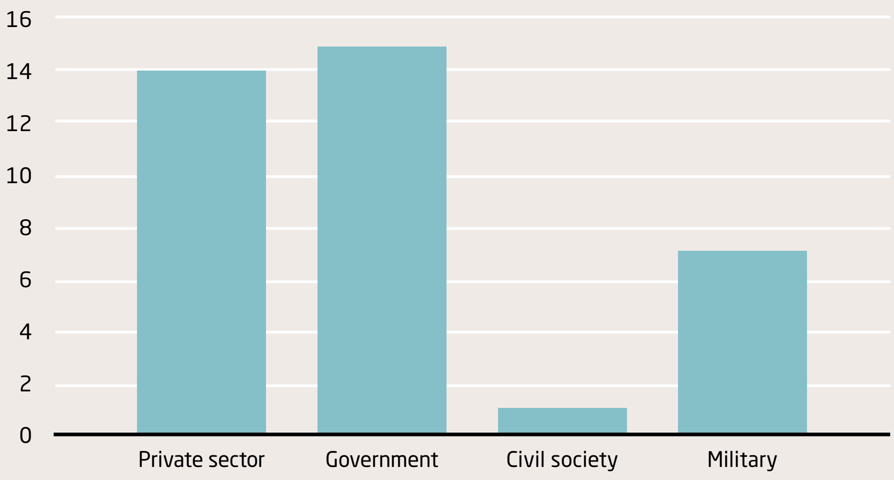
Of 23 publicly known cyberattacks originating from China targeting Europe since 2005, as tracked by the Council of Foreign Relations, the majority were aimed at government institutions. All were classified as "espionage."

A recent EU document highlighting potential attacks on digital infrastructure and information systems in the upcoming May 2019 elections to the European Parliament elections in May 2019 primarily refers to risks from Russia.[84] However, the growing evidence of Chinese authorities cultivating Europe's right-wing populist parties suggests a potential cyber-attack on EU or European digital services during the 2019 poll cannot be ruled out. The risks can only grow in the medium term, based on evidence about China's cyber activities in its nearer neighborhood.[85] (see exhibit 14).

Exhibit 14

Chinese hackers focus on political institutions

Cyberattacks on Europe by target sector



Source: Council of Foreign Relations (2018). "Cyber Operations Tracker". https://www.cfr.org/interactive/cyber-operations. Accessed: October 22, 2018

© MERICS

4.4 EUROPE NEEDS TO TACKLE THE CHALLENGES ARISING FROM CHINA'S SOCIAL CREDIT SYSTEM

The Social Credit System seems likely to affect human security negatively, a term that is at the heart of how the EU conceptualizes security since the 1990s. It is still in the testing and build-up phase,[86] so it is too early for a full picture. Nonetheless, it is certain that the Social Credit System will pose challenges for the EU and European actors. European citizens' privacy, safety and rights need protection from Chinese government encroachment. This includes protection from European commercial actors that may cooperate with China's authorities.

On present knowledge, EU citizens who live in China long-term will be integrated into the Social Credit System, individually and, where applicable, as the legal representative of a company. Data about them will be systematically collected and aggregated in a central repository.

Chinese companies operating in Europe could collect and use data on EU citizens – and others – within EU territory, inside the permissible legal framework. There is the further risk that Chinese companies (such as Baidu, Alibaba, or Tencent) and internationally listed companies operating in China could be pressured to collect and hand over data to the Chinese government beyond what is permitted by the European legal framework.

Finally, data on violations of China's political regulations by foreign companies and NGOs operating in China (and potentially their parent organizations abroad) could be stored under social credit records and later used to pressure foreign entities into complying with Chinese censorship.

Even if China were to introduce regulations restricting government use of data, any agreement between China and the EU on data transfer should be weighed carefully, given the lack an independent judiciary able to enforce regulations against CCP interests.

China's as yet limited efforts to establish a data protection regime fail to cover abuse or unchecked data collection by government actors. Protecting citizens from government overreach is not discussed – and cannot be discussed – in China's current political climate. However, the Social Credit System can be applied to force compliance with vague, politically motivated regulations.[87]

China's limited efforts to establish a data protection regime fail to cover abuse by government actors

The overall normative effect of a successful and exportable social credit system is a serious challenge to what is considered acceptable digital ethics in Europe. The Social Credit System and related regulations could be emulated by non-European actors and even – in part, and in a modified form – within Europe itself.

The Social Credit System subsumes various sub-systems, some of which show substantial convergence with what individual European countries are doing in some areas.[88] European actors need to be vigilant against accusations that European initiatives for assessing citizens creditworthiness (Germany) or their welfare state abuses (Netherlands) are similar to those envisioned by China's Social Credit System. However, China's government-commissioned local pilots to develop comprehensive ratings for individual citizens go far beyond anything that would be legally possible in Europe (see exhibit 15).

Exhibit 15

China's cyber governance is also targeting foreign citizens

Type of project and impact by target

Project	Individuals affected	Companies affected	Foreigners in China	Foreign companies in China
Unified Social Credit Number An 18-digit number to act as a "single indentity" in China	Yes (same as national ID; already in place)	Yes	Not yet	Yes
Central databases Central data repositories to quickly retrieve information related to "trustworthiness"	Yes	Yes	In theory	Yes, but uneven implementation
National black lists System to publicize and punish those who have violated regulations	Yes (for debt defaulter)	Yes (IPR violations, pyramid schemes, unsafe production, etc.)	Yes (for debt defaulters, plus no fly/no HSR list)	Yes, but uneven implementation
Joint rewards and punishments system System to exchange information to make sure blacklisted individuals and entities are restricted across bureaucracies	Yes, e.g. through • Travel restrictions • Additional restrictions on high-end consumption (e.g. certain hotel classes) • Public shaming	Yes, e.g. through • Restrictions in government procurement • Intensified monitoring • Travel restrictions for legal representatives • Public shaming	Yes, in theory	Yes, but uneven implementation
Nationwide scoring Comprehensive scores assess individuals or legal entities across a number of different criteria and assign a single score	No	Yes, for specific areas (taxes, customs, etc.), but no comprehensive score	No	Yes, for specific arenas (taxes, customs, etc.), but no comprehensive score
Commercial scoring pilots Non-licensed commercial pilot projects assign scores to users using aggregated data and unspecified algorithms	Yes, but not mandatory	Yes, for specific areas (taxes, customs, etc.), but no comprehensive score	Yes, but not mandatory	Possibly, but not mandatory
Local scoring pilots Comprehensive scores assess individuals or legal entities across a number of different criteria and assign a single score	Yes, in several cities	Yes, in several cities and provinces	In theory	Yes

Source: MERICS

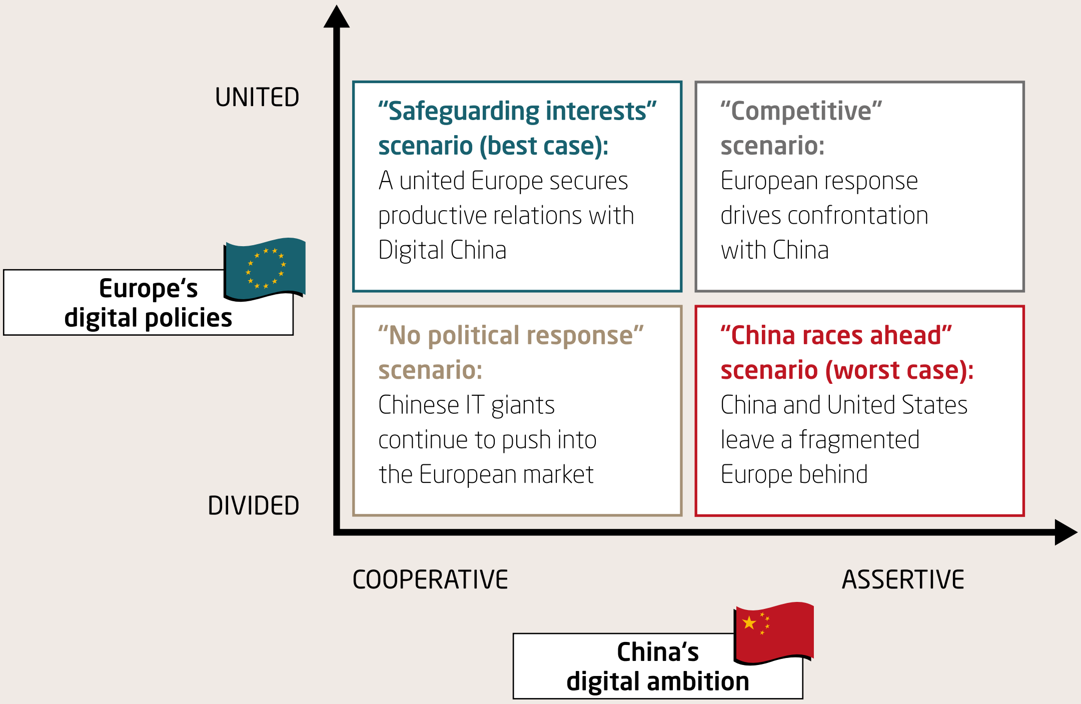
5. Outlook: Managing competition in a digital age

China's digital ambitions will not play out along a linear trajectory. The disruptive nature of the technology itself and the geo-economic and political environment in which it develops can reinforce or undermine conscious choices by both Beijing and Brussels. The way China's digital rise will affect Europe will, first and foremost, depend on two critical, overarching conditions, namely whether:
1) Beijing pursues its digital ambitions within a politically more assertive or cooperative framework; and/or
2) Europe responds to the challenges from China's digital rise in a united and strong or fragmented and therefore weak manner.

Taking into account these conditions, Europe might find its relationship with China on digital matters evolves within one or several of four conceivable scenarios:

Exhibit 16

China's digital rise will affect Europe
A look into possible future trajectories



"Safeguarding interests" scenario (best case): A united Europe secures productive relations with Digital China

"Competitive" scenario: European response drives confrontation with China

"No political response" scenario: Chinese IT giants continue to push into the European market

"China races ahead" scenario (worst case): China and United States leave a fragmented Europe behind

Source: MERICS

The scenarios in the matrix above show that at present there is considerable uncertainty about future relations between China and Europe in the digital sphere. The future depends on several factors: on political-economic dynamics in China; on the degree of internal European alignment on digital policies; on the development of Europe's own digital industry base; and on China and Europe's relationships with the United States.

Best case: a united Europe safeguards its interests vis-à-vis Digital China

In this scenario, Europe manages to minimize risks and safeguard balanced and reciprocal conditions in its relations with China. The scenario would require a willingness from Beijing to pursue more substantive market reforms, i.e. ending massive state support and guidance for China's big IT champions, as well as enhanced intellectual property and data protection. Beijing is more likely to commit to economic liberalization and legal enforcement if China's IT companies still depend upon foreign tech components and need international collaboration to achieve their ambitions to develop high-tech and emerging technologies.

On the EU side, the member states would need to synchronize their regulatory frameworks to enhance the Digital Single Market, and to strengthen and reform instruments for trade defense and fair competition. The European continent would need to build up a more competitive digital industry, putting Europe in a better positioned to advocate for its core strengths, i.e. data privacy and ethical standards.

In this scenario, China's strength in creating digital business models and multi-faceted platforms has the potential to complement European companies' technological edge in smart manufacturing or industrial AI and in the production of high-quality IoT components.

"No political response" scenario: China's IT giants continue their push into Europe

Chinese ICT companies can be expected to continue making inroads into European markets by securing online payment licenses or by buying into smart city projects.

China's government is likely to continue its support for domestic IT companies. Furthermore, privately-held enterprises linked to Alibaba or Tencent and emerging start-ups will seek to expand abroad. For emerging digital companies, China's domestic digital market is highly distorted, competitive and fast-paced; it pushes players to gain experience and to capture market share and customers abroad in order to survive.

In this scenario, European companies would seek cooperation with Chinese counterparts to gain access to an attractive market with laxer customer data regulations, attractive testing facilities and pilot projects. As a result, Chinese companies would become an integral part of transnational digital networks and ecosystems.

The EU and its member states need to adapt their decision making to the fast pace of digitalization, otherwise developments on the ground are likely to outpace attempts at regulation.

"Competitive" scenario: European responses drive confrontation with China

A more coherent and increasingly tough EU policy vis-à-vis China could lead to fierce competition and possibly confrontation.

Given the considerable pressure the CCP is facing from China's continuing economic slowdown, Beijing is likely to double down on its efforts to become self-reliant and a global leader in digital technologies. China's government will continue its assertive digital policy by subsidizing and protecting domestic IT champions, including their international outreach activities. China's economic and political cyber espionage is likely to increase.

The EU already is becoming more aware of the heightened competition and challenges arising both from China's tech nationalism and its promotion of alternative models of governance. If it switches from just more pro-active strategies into protective measures, i.e. against China's advances into critical infrastructure, this could fuel an even more assertive answer from Beijing.

On a global level, the EU's more protective approach towards data privacy and digital ethics could set Europe apart from the data-greedy models pursued in China and hence become a key building block in creating a European competitive edge in digitalization.

Competition for talent could become another key area of confrontation. Although Europe still scores more highly for attractive research environments and living standards, Chinese companies may attract increasing numbers of professionals with monetary incentives and rapid career trajectories.

Worst case: China leaves Europe behind in the digital sphere

If Europe fails to come up with an EU-wide digital agenda and build a competitive tech industry base, it could well be left trailing behind a strong digital China that has succeeded in achieving global leadership in key technologies.

In this scenario, Beijing could succeed in overcoming its most pressing economic challenges and go on to achieve an effective balance between better-targeted state support and an increase in the size of the private ITC sector supported by venture capital. China could then be better-positioned to achieve self-reliance and international leadership in technologies like quantum or AI.

Meanwhile, the EU member states' digital policies are likely to remain dominated by nationalist and protectionist tendencies. Europe would then risk being left behind as a contributor to the digitalization of the global economy and society – and, first and foremost, to their own digital ecosystems.

If Europe lacks competitive home-grown tech solutions, for instance to equip its future telecommunications infrastructure, it risks becoming over dependent on products from China – or the United States, for that matter. As a result, Europe's digital landscape would be one of fragmented, not necessarily inter-operable, digital infrastructures and ecosystems dominated by Chinese or US actors. Reliance on components from foreign supplies would leave Europe facing increased vulnerability in critical infrastructure, such as smart energy or traffic networks.

Facing the competitive challenge in the US-China-EU triangle

Whether Europe will succeed in the digital age also depends on relations with its lately increasingly difficult ally, the United States. The Trump administration's "America first" policy hampers closer cooperation in the digital sphere.

European nations are already caught up in a protracted and structural US-China conflict: Washington increasingly views China as a strategic competitor and an adversary, both from an economic perspective and in geopolitical and security issues.

Nonetheless, if the EU's relations with the United States remain frosty, the continent risks becoming permanently caught between a rock and a hard place and having to deal with a fragmented digital world ruled by Chinese or US tech solutions. Homegrown European products may be unable to compete internationally. The US campaign to push back against the deployment of Huawei technology in Europe is a foretaste of possible future conflicts.

However, the United States, the EU and its member states have more common interests when it comes to managing and developing the digital realm than any of them do with China, not least because they share democratic systems and values. China's digital outreach is not solely driven by economic motives. It is also fundamentally linked to competition between systems, and China's differences with the principles of the liberal market economy, free trade and liberal democracy. Europe has to brace itself for these challenges.

RECOMMENDATIONS: VIGILANCE, UNITY AND LEVERAGE ARE NEEDED TO PREVAIL IN THE DIGITAL WORLD

Digital China is challenging Europe on several levels. Opportunities for collaboration certainly exist in some areas. However, in others Europe should not delay taking action to safeguard its interests in a fast changing economic and technological environment:

Strengthening Europe

- **Double-down on a European strategically autonomous digital policy.** Support new financing vehicles to strengthen Europe's digital industry sector, facilitate market-orientated joint research, expand the digital market by supporting cross border business solutions, further harmonizing digital standards and legislation. Prepare for increasing US pressure and potential intra-EU divergence on digital (dis-)entanglement with China.
- **Strengthen a joint approach to cyber security across Europe, specifically with a view to reducing strategic dependence in critical infrastructure.** Take the European Commissions' recommendations on a common approach to security of 5G networks as a blueprint to develop joint risk assessment and risk management measures and sanction mechanisms to counter cyber-attacks.
- **Facilitate close cooperation and information exchange between EU member states on Chinese tech companies' advances in critical infrastructure** (e.g. via DG Connect, EU INTCEN and/or ENISA). In light of substantial uncertainties related to the deployment of 5G infrastructure by Chinese suppliers, European member states and the Commission need to align their position to prevent a digital split across Europe.
- **Consider ways to make EU digital market access for Chinese investors conditional using regulatory measures.** Create leverage for reciprocal market access on European terms.
- **Close loopholes in Europe-wide export controls to ensure European companies are not implicated in building China's surveillance state, including beyond its borders.** Address the implications of the export of Chinese surveillance systems, especially in developing countries, in regard to protection of citizens' rights and good governance.
- **Monitor China's civil-military integration drive in innovation capacities and the implications for dual-use tech and research cooperation.** Prevent enhancing China's surveillance and military capacities by monitoring joint research projects.
- **Systematically track China's weaknesses and dependencies as revealed through adjustments to national policy plans and accessible experts' online debates.** Identify potential weak spots and internal disagreements to leverage European advantages and press for beneficial terms of cooperation.
- **Establish a "Europe-China Economic Strategy and Digital Futures Task Force" to help coordinate China policy across DGs and member states.** The Task Force should be capable of commissioning targeted short-term research projects to develop recommendations and facilitate exchanges among stakeholders in Brussels, key member states and industry. It could also serve as a high-level counterpart for related Track 1.5 exchanges with allies and vis-a-vis China.

Engaging with China

- **Call out China's actors when the PRC's domestic cyber regulations directly or indirectly infringe the privacy of European economic actors' and citizens.** Monitor the impact of the evolving social credit system, including beyond China's borders. Be vigilant towards possible forced data transfer by Chinese digital services companies responding to pressures from China's national security bodies.
- **Seek targeted coordination with China on EU terms, where appropriate** (e.g. IoT standards or industrial AI). Safeguard ethical standards and data protection, putting the EU's strengths to the fore in shaping cooperation
- **Define and communicate "red lines" as well as exit options for joint research projects between China and Europe.** Make sure to guarantee European participants equal access to data and equal rights to publish results.
- **Prioritize digital issues (cross-border data flows, e-commerce, cyber security etc.) in ongoing negotiations and discussions with China about the future of the multilateral trading system and the EU-China investment agreement.**

Engaging with third countries

- **Seek global normative leadership by continuously addressing legal problems and ethical issues created by new digital technologies.** This should include big data and AI, data protection and safe data flows, transparency requirements for algorithms that rate and assess individuals, data manipulation, data discrimination, etc. The General Date Protection Regulation (GDPR) should be more actively promoted as the trademark of Europe's sustainable and inclusive approach to regulation in the digital realm.
- **Seek greater alignment with the US and other member states of the "Five Eyes" intelligence alliance and with advanced economies like South Korea or Japan.** Push back jointly against China's subsidized industrial policy and its emphasis on indigenous innovation that fosters digital protectionism. Rapidly expand work with like-minded partners towards agreements on privacy, data localization and cyber standards, as well as free and safe data flows.
- **Strengthen joint work on the application of existing international law to the behavior of states in cyberspace as well as cyber security standards.** Build on the newly acquired permanent mandate for EU cyber security given to ENISA (EU Agency for Network and Information Security) as part of the EU Cybersecurity Act.
- **Actively promote the EU "Connectivity Strategy" as a more locally beneficial and sustainable alternative to the "Digital Belt and Road" globally.** European digital connectivity should be actively advanced especially across Eastern Europe and the Balkans. European participation on projects related to China's "Digital Belt and Road Initiative" should be approached cautiously.

Endnotes:

[1] Hooker, Lucy and Palumbo, Danilo (2018). "Huawei: The Rapid Growth of a Chinese Champion in Five Charts." BBC News. December 7. https://www.bbc.com/news/business-46480208. Accessed: February 28, 2019.

[2] Ding, Jeffrey (2018). "Deciphering China's AI Dream." March. https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf. Accessed: November 30, 2018.

[3] Wübbeke, Jost et al. (2016). "Made in China 2025." MERICS Papers on China. December. https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf. Accessed: November 30, 2018.

[4] Nouwens, Meia and Legarda, Helena (2018). "China's Pursuit of Dominance in Dual-Use Technologies. Implications For Europe." International Institute for Strategic Studies. December 18. https://www.iiss.org/blogs/analysis/2018/12/emerging-technology-dominance. Accessed: January 30, 2019.

[5] Tao, Li (2018). "How China's 'Big Fund' is Helping the Country Catch up in the Global Semiconductor Race." SCMP [South China Morning Post]. May 10. https://www.scmp.com/tech/enterprises/article/2145422/how-chinas-big-fund-helping-country-catch-global-semiconductor-race. Accessed: September 19, 2018.

[6] Wübbeke, Jost et al. (2016). "Made in China 2025." MERICS Papers on China. December. https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf. Accessed: September 10, 2018.

[7] Wang, Huiyao (2010). "China's National Talent Plan: Key Measures and Objectives." Brookings Report. November 23. https://www.brookings.edu/research/chinas-national-talent-plan-key-measures-and-objectives/. Accessed: March 25,2019.

[8] Ding, Jeffrey (2018). "Deciphering China's AI Dream." University of Oxford. March. https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream-1.pdf. Accessed: March 25, 2019.

[9] Bien Perez, Bien (2017). "Why China is Set to Spend US$411 Billion on 5G Mobile Networks." June 19. https://www.scmp.com/tech/china-tech/article/2098948/china-plans-28-trillion-yuan-capital-expenditure-create-worlds. Accessed: March 30, 2019; Hisilicon (2018). "Huawei Releases First 5G Customer-Premises Equipment." February 25. http://www.hisilicon.com/en/Media-Center/News/Huawei%20Releases%20First%205G%20Customer-premises%20Equipment. Accessed: March 27,2019; Kharpal, Arjun (2018). "China 'Has the Edge' in The War for 5G And The US And Europe Could Fall Behind." March 7. https://www.cnbc.com/2018/03/07/china-has-the-edge-in-the-war-for-5g-us-and-eu-could-fall-behind.html. Accessed: March 30,2019; Hedge, Zenobia (2018). "Five Reasons Why Europe Has Already Lost the 5G Race." June 21. https://www.iot-now.com/2018/06/27/84975-five-reasons-europe-already-lost-5g-race/. Accessed: March 25, 2019.

[10] Lee, Stacia (2017). "The Cybersecurity Implications of Chinese Undersea Cable Investment." February 6. https://jsis.washington.edu/eacenter/2017/02/06/cybersecurity-implications-chinese-undersea-cable-investment/. Accessed: March 25, 2019.

[11] Schenker, Jennifer L. (2018). "Why China Wants To Lead The 5G Charge." March. https://innovator.news/why-china-wants-to-lead-the-5g-charge-249151bee73b. Accessed: March 25, 2019.

[12] Smith, Rob (2018). "42% of Global E-Commerce is Happening in China. Here's Why." World Economic Forum. April 18. https://www.weforum.org/agenda/2018/04/42-of-global-e-commerce-is-happening-in-china-heres-why/. Accessed: March 31, 2019.

[13] See Pasquier, Martin (2015). "Internet Plus: China's Official Strategy for the Uberisation of the Economy." May 2015. https://www.innovationiseverywhere.com/internet-plus-chinas-official-strategy-for-the-uberisation-of-the-economy/. Accessed: October 30, 2018.

[14] Fortune (2018). "U.S. Puts Alibaba's Taobao on Blacklist for Counterfeit Products — Again." January 12. http://fortune.com/2018/01/12/alibaba-taobao-blacklist-counterfeit-products/. Accessed: September 20, 2018.

[15] Personal interviews at a workshop on the evolvement of the Chinese e-commerce law organized by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) in Berlin in spring 2017.

[16] NPC Observer (2018). "E-Commerce Law of the People's Republic of China." https://npcobserver.com/lawlist/e-commerce-law/. Accessed: September 18, 2018

[17] Dickinson, Steve (2018). "New Restrictions on High Tech Technology Transfers to China." China Law Blog. November 27. https://www.chinalawblog.com/2018/11/new-restrictions-on-high-tech-technology-transfers-to-china.html. Accessed: November 30, 2018.

[18] Chen, Yawen (2018). "China's city of Tianjin to set up $16-billion artificial intelligence fund". Reuters. May 17. https://www.reuters.com/article/us-china-ai-tianjin/chinas-city-of-tianjin-to-set-up-16-billion-artificial-intelligence-fund-idUSKCN1II0DD. Accessed: October 15, 2018.

[19] Deloitte (2018). "5G: The Chance to Lead for a Decade." https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf. Accessed: October 15, 2018.

[20] Laskai, Lorand (2018). "Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies Publication." China Brief Volume 18, Issue 6. April 9. https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/. Accessed: March 28, 2019.

[21] Huang, Eli (2017). "China's Cable Strategy: Exploring Global Undersea Dominance." December 4. http://www.theworldin.com/article/14433/edition2018digital-silk-road. Accessed: February 11, 2019; Wilson, Jordan (2017). "China's Alternative to GPS and its Implications for the United States." U.S.-China Economic and Security Review Commission. January 5. https://www.uscc.gov/sites/default/files/Research/Staff%20Report_China%27s%20Alternative%20to%20GPS%20and%20Implications%20for%20the%20United%20States.pdf. Accessed: March 25, 2019.

[22] Russel, Jon (2018). "Alibaba Doubles Down on Lazada with Fresh $2B Investment And New CEO." TechCrunch. March 18, 2018. https://techcrunch.com/2018/03/18/alibaba-doubles-down-on-lazada/?guccounter=1. Accessed: September 25, 2018.

23 | Shen, Hong (2018). “Building a Digital Silk Road? Situating the Internet in China’s Belt and Road Initiative.” International Journal of Communication 12: 2683–2701.

24 | National Development and Reform Commission 中华人民共和国国家发展和改革委员会 (2015). ”《标准联通“一带一路”行动计划（2015–2017）》发布. ” [Publication of the “Action Plan for Harmonization of Standards Along ‘Belt and Road Initiative’ (2015-2017)]. October 22. http://www.ndrc.gov.cn/xwzx/xwfb/201510/t20151022_755476.html. Accessed: October 18, 2018.

25 | STDaily 国际科技频道 (2018). “我国“抢”得国际物联网领域话语权.” [China “Grabs” the Global Discourse Power in the Internet of Things Realm]. July 11. http://www.stdaily.com/guoji/xinwen/2018-07/11/content_689184.shtml. Accessed: October 16, 2018.

26 | de Jong-Chen, Jing and O’Brien, Bobby (2017). “Approach to Critical Infrastructure Protection in the U.S., E.U., and China.” Wilson Center. November 14. https://www.wilsoncenter.org/publication/comparative-study-the-approach-to-critical-infrastructure-protection-the-us-eu-and-china. Accessed: December 8, 2018.

27 | Cook, Sara (2018). “China’s Cyber Superpower Strategy: Implementation, Internet Freedom Implications, And U.S. Responses.” Freedom House. September 26. https://oversight.house.gov/wp-content/uploads/2018/09/Cook-FreedomHouse-Statement-China-9-26.pdf. Accessed: September 30, 2018.

28 | Triolo, Paul et. al. (2017). “China’s Cybersecurity Law One Year On.” New America. November 20. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/. Accessed: September 30, 2018.

29 | Additional draft regulations issued in July 2017 explicitly added news media, healthcare, cloud computing and big data providers, see: Triolo, Paul, Creemers, Rogier, and Webster, Graham (2017). “China’s Ambitious Rules to Secure ‘Critical Information Infrastructure.’” New America. July 14. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/. Accessed; September 27, 2018.

30 | Cyberspace Administration of China (AC) (2017). “关于发布《网络关键设备和网络安全专用产品目录(第一批)》的公告. ” [Announcement on the Promulgation of the Catalog of Key Network Equipment and Specific Network Safety Products (Batch One)] June 9. http://www.cac.gov.cn/2017-06/09/c_1121113591.htm. Accessed: September 29, 2018.

31 | KPMG (2017). “Overview of China’s Cybersecurity Law.” February. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf. Accessed: September 27, 2018.

32 | Some foreign companies are already facing pressure for complying with this law. For instance, Apple’s China iCloud services have been managed by Guizhou-Cloud Big Data, which has close ties to the government. Even if companies do not hand data over voluntarily, there is a still a risk of data leaks. Some companies, such as Asus, have decided to withdraw entirely from China’s cloud storage market due to privacy and security concerns. The data localization requirements also put Chinese companies wanting to enter global markets under pressure as they have to navigate different data protection regimes, see: Liao, Shannon (2018). “Apple Officially Moves its Chinese iCloud Operations and Encryption Keys to China.” The Verge. February 12. https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed. Accessed: October 12, 2018; Huang, Paul (n.d.). “In Sharp Contrast to Apple, Asus Bows Out of China’s Cloud Storage Market to Protect Private User Data.” https://codecprime.com/partner/content/2254274-sharp-contrast-apple-asus-bows-out-china-s-cloud-storage-market-protect-private-user. Accessed: November 22, 2018.

33 | Gao, Charlotte (2018). “China’s Great Firewall: A Serious Pain in the Neck for European and US Companies.” The Diplomat June 21, https://thediplomat.com/2018/06/chinas-great-firewall-a-serious-pain-in-the-neck-for-european-and-us-companies/. Accessed: November 30, 2018.

34 | Chan, Tara Francis (2018). “It Looks Like China is Extending its Black Mirror-like ‘Social Credit System’ to Overseas Companies.” Business Insider. July 3. https://www.businessinsider.de/china-social-credit-system-controlling-foreign-companies-2018-6?r=US&IR=T. Accessed: September 8, 2018.

35 | Huang, Zheping (2017). „China Wants to Build a Credit Score that Dings Online Chat Group Users for Their Political Views.” Quartz. September 8. https://qz.com/1072660/china-wants-to-build-a-credit-score-that-ings-online-chat-group-users-for-their-political-views/. Accessed: December 12, 2018.

36 | The Economist (2018). “China’s Great Firewall is Rising.” January 4. https://www.economist.com/china/2018/01/04/chinas-great-firewall-is-rising. Accessed: September 24, 2018.

37 | Eurasia Group (2018): “The Geopolitics of 5G.” November 15. https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf. Accessed: November 6, 2018.

38 | Deloitte (2018). “5G: The Chance to Lead for a Decade.” https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf. Accessed: October 15, 2018.

39 | Ernst&Young, EY (2018). “EY Releases New Report: China is Poised to Win the 5G Race.” June 13. https://www.ey.com/cn/en/newsroom/news-releases/news-2018-ey-releases-new-report-china-is-poised-to-win-the-5g-race. Accessed: January 6, 2019.

40 | Eisenstark, Roma (2018). “Why China And The US Are Fighting Over 5G.” Technode. March 30. https://technode.com/2018/03/30/5g/ . Accessed: January 10, 2019.

41 | Kania, Elsa (2017). “China’s Artificial Intelligence Revolution.” The Diplomat. July 27. https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/. Accessed: March 13, 2019.

42 | Chen, Yawen (2018). “China’s City of Tianjin to Set up $16-Billion Artificial Intelligence Fund.” Reuters. May 17. https://www.reuters.com/article/us-china-ai-tianjin/chinas-city-of-tianjin-to-set-up-16-billion-artificial-intelligence-fund-idUSKCN1II0DD. Accessed: October 15, 2018.

43 | Okoshi, Yuki (2019). “China Overtakes US in AI Patent Ranking.” Nikkei Asian Review. March 10. https://asia.nikkei.com/Business/Business-trends/China-overtakes-US-in-AI-patent-rankings. Accessed: March 12, 2019; Diamandis, Peter H. (2018). “China is Quickly Becoming an AI Superpower.” SingularityHub. August 29. https://singularityhub.com/2018/08/29/china-ai-superpower/#sm.0000vx96wm5h5duvye42h-74g8kc46. Accessed: November 14, 2018.

44 | Okoshi, Yuki (2019). "China Overtakes US in AI Patent Ranking." Nikkei Asian Review. March 10. https://asia.nikkei.com/Business/Business-trends/China-overtakes-US-in-AI-patent-rankings. Accessed: March 12, 2019. Diamandis, Peter H. (2018). "China is Quickly Becoming an AI Superpower." SingularityHub. August 29. https://singularityhub.com/2018/08/29/china-ai-superpower/#sm.0000vx96wm5h5duvye42h74g8kc46. Accessed: November 14, 2018.

45 | Chen, Celia (2018). "China's Artificial Intelligence Sector in Danger of Becoming a 'Bubble', Experts Warn." SCMP [South China Morning Post]. March 26. https://www.scmp.com/tech/innovation/article/2082217/chinas-artificial-intelligence-sector-danger-becoming-bubble-experts. Accessed: September 1, 2018.

46 | Benaim, Daniel (2018). "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders." Slate. August 9. https://slate.com/technology/2018/08/chinas-export-of-cutting-edge-surveillance-and-facial-recognition-technology-will-empower-authoritarians-worldwide.html. Accessed: October 18, 2018.

47 | "Initial Coin Offerings" are the most common ways for blockchain companies to raise funds, similar to "Initial Public Offering" (IPO) for conventional companies. These ICOs were particularly rampant in China. Wen, Jing 文静 (2018) "中国严禁ICO，从法律层面解读虚拟货币" [China bans ICOs and gives cryptocurrencies a legal interpretation]. Caijing. September 4. http://yuanchuang.caijing.com.cn/2018/0904/4509910.shtml. Accessed: February 19. 2019.

48 | Wen, Fan (2018). Blockchain Start-Ups (2000-2018). October 28. https://public.tableau.com/profile/fan.wen5373#!/vizhome/Blockchain_Companies/MapofStartups. Accessed: February 17, 2019.

49 | Amsili, Miryam (208). "Blockchain In China: Local Is Everything." Supchina. August 28. https://supchina.com/2018/08/28/blockchain-in-china-local-is-everything/. Accessed: February 18, 2019.

50 | PwC (2018b). "Blockchain is Here. What's Your Next Move?". https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html. Accessed: February 20, 2019.

51 | International Data Corporation, IDC (2018). "Worldwide Spending on Blockchain Forecast to Reach $11.7 Billion in 2022. According to New IDC Spending Guide." July 19. https://www.idc.com/getdoc.jsp?containerId=prUS44150518. Accessed: February 23, 2019.

52 | Deloitte (2018). "Breaking Blockchain Open." https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf. Accessed: February 21, 2019.

53 | PricewaterhouseCoopers, PwC (2018a). "2018 Market Survey Report for (Non-financial) Application of Blockchain in China." https://www.pwccn.com/en/risk-assurance/2018-china-blockchain-survery-report-en.pdf. Accessed: February 21, 2019.

54 | Letzter, Rafi (2018). "China's Quantum-Key Network, the Largest Ever, Is Officially Online." LiveScience. 19 January. https://www.livescience.com/61474-micius-china-quantum-key-intercontinental.html. Accessed: February 17, 2019; Leary, Kyree (2018). "Quantum Video Call Displays the Future of Secure Communication." Futurism. February 2. https://futurism.com/quantum-video-secure-communication. Accessed: February 20, 2019.

55 | Meghji, Sultan (2016). "Has the Battle for Quantum Supremacy Already Been Lost?" Medium. September 18. https://medium.com/@sultanmeghji/has-the-battle-for-quantum-supremacy-already-been-lost-19619a36627b. Accessed: January 23, 2019.

56 | The Heritage Foundation (2019). "Quantum Science and National Security: A Primer for Policymakers." February 5. https://www.heritage.org/node/10888847/print-display. Accessed: February 10, 2019.

57 | Chen, Stephen (2018). "China Building World's Biggest Quantum Research Facility." South China Morning Post. July 20. https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility. Accessed: February 23, 2019.

58 | Kanina, Elsa and Costello, John (2018). "Quantum Hegemony". September. https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406. Accessed: February 2, 2019.

59 | Kanina, Elsa and Costello, John (2018). "Quantum Hegemony". September. https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406. Accessed: February 2, 2019.

60 | Legarda, Helena and Nouwens, Meia (2018). "China's Pursuit of Advanced Dual-Use Technologies-" The International Institute for Strategic Studies, IISS. December 18. https://www.iiss.org/blogs/analysis/2018/12/emerging-technology-dominance. Accessed: February 2, 2019.

61 | Miller, Matthew (2018). "Huawei Announces Watch GT and Band 3 Pro: Made for Urban Explorers as Companions to the Mate 20 Series." ZDNet. October 16, 2018. https://www.zdnet.com/article/huawei-announces-3b-uk-procurement-plan. Accessed: October 18, 2018; Haier (2018). "Haier CosmoPlat at Hannover Messe 2018." Haier Global. April 26. https://haierglobal.blogspot.com/2018/04/haier-cosmoplat-at-hannover-messe-2018.html. Accessed: September 20, 2018.

62 | Veugelers, Reinhilde (2017a). "Countering European Brain Drain." Science 356 (6339): 695-696.

63 | Veugelers, Reinhilde (2017b). "The Challenge of China's Rise as a Science and Technology Powerhouse." Bruegel Policy Contribution. July. http://bruegel.org/wp-content/uploads/2017/07/PC-19-2017.pdf. Accessed: March 14, 2019.

64 | European Supermarket Magazine (2018). "Alibaba Signs Deal To Open 'Smart Logistics Hub' In Liege, Belgium." December 10. https://www.esmmagazine.com/alibaba-signs-deal-open-smart-logistics-hub-liegebelgium/68540. Accessed on December 12, 2018; Harris, David (2017). "What is eWTP, And Why You Should Care." January 4. https://cargofacts.com/what-is-ewtp-and-why-you-should-care/. Accessed on December 12, 2018.

65 | Yang, Yuan (2019). "Is Huawei Compelled by Chinese Law to Help With Espionage?" Financial Times. March 4. https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0. Accessed: March 5, 2019.

66 | HCSEC [Huawei Cyber Security Evaluation Centre Oversight Board] (2018). "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2018." National Security Adviser. July. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018. Accessed: October 4, 2018.

67 | The Straits Times (2018). "China Outnumbers Other Countries in Smart City Pilots: Report." February 20. https://www.straitstimes.com/asia/east-asia/china-outnumbers-other-countries-in-smart-city-pilots-report. Accessed: October 15, 2018.

68 | Hoffmann, Samantha (2018). "Technology-Enhanced Authoritarian Control With Global Consequences." Australian Strategic Policy Institute. June 28. https://www.aspi.org.au/report/social-credit. Accessed: September 28, 2018; Hofmann, Samantha (2018). "Grasping Power With Both Hands: Social Credit, the Mass Line, and Party Control." https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control/. Accessed: October 17, 2018.

69 | China Economic Net中国经济网 (2013). "智慧城市助力社会管理创新. " [Smart Cities Support Social Management Innovation] July 8. http://views.ce.cn/view/ent/201307/08/t20130708_24548958.shtml. Accessed: October 2, 2018.

70 | Mozur, Paul (2018). "Looking Through the Eyes of China's Surveillance State." New York Times. July 16. https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html. Accessed: September 20, 2018.

71 | Carner, Matthew (2018). "Leave no Dark Corner." ABC News. September 17. https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278. Accessed: October 5, 2018.

72 | Bürge, Clément (2017). "Life Inside China's Total Surveillance State." Wall Street Journal. December 19. https://www.wsj.com/video/life-inside-chinas-total-surveillance-state/CE86DA19-D55D-4F12-AC6A-3B2A573492CF.html. Accessed: October 8, 2018.

73 | Presseportal (2018). "Huawei vertieft Kooperation mit Duisburg, um den deutschen Industriestandort in eine neue Smart City zu verwandeln." [Huawei strengthens cooperation with the city of Duisburg to help the German industry hub transform into a Smart City]. September 9, 2018. https://www.presseportal.de/pm/100745/4051263. Accessed: October 12, 2018.

74 | Xinhua 新华 (2018). "Malta, Huawei sign 5G Infrastructure Agreement." July 14. http://www.xinhuanet.com/english/2018-07/14/c_137324156.htm. Accessed: October 14, 2018.

75 | Huawei (2016). "Huawei Signs Smart City Project Agreement at Its Global Safe City Summit at CeBIT 2016." March 17. https://www.huawei.com/en/press-events/news/2016/3/smart-city-project. Accessed: September 28, 2018.

76 | Huawei (2018). "Huawei Safe City Solution: Safeguards Serbia." https://e.huawei.com/en/case-studies/global/2018/201808231012. Accessed: September 28, 2018.

77 | Alibaba (2018). "Alibaba Cloud and ABC Data Enter into Strategic Partnership." August 21. https://www.alibabacloud.com/de/press-room/alibaba-cloud-and-abc-data-enter-into-strategic-partnership. Accessed: October 10, 2018.

78 | European Commission (2013). "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions." February 2. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. Accessed: October 2, 2018.

79 | Desvignes, Frank (2016). "The Internet of Things – Made in China." AxA. October 5. https://www.axa.com/en/spotlight/story/internet-of-things-made-in-china. Accessed: September 12, 2018.

80 | Boddy, Sara and Shattuck, Justin (2017). "The Hunt for IoT." F5labs. February. https://www.f5.com/content/dam/f5/downloads/F5_Labs_Hunt_for_IoT_Vol_2_rev_11JUL17.pdf. Accessed: October 15, 2018.

81 | EU (2018). "The EU-China Study on IoT and 5G." EU's Horizon2020. https://www.euchina-iot5g.eu/about/. Accessed: October 2, 2018. Among European companies, the only substantial industrial partnership to co-develop IoT solutions is between Bosch and Huawei, but its focus is to offer Bosch IoT software on a Huawei Cloud in China.

82 | From 2005 to October 2018, 23 incidents have been recorded for Europe vs. 67 for the United States. Council of Foreign Relations (2018). "Cyber Operations Tracker." https://www.cfr.org/interactive/cyber-operations. Accessed: October 22, 2018.

83 | Farley, Robert (2018). "Did the Obama-Xi Cyber Agreement Work?" The Diplomat. August 11. https://thediplomat.com/2018/08/did-the-obama-xi-cyber-agreement-work/. Accessed: October 17, 2018.

84 | European Commission (2018), "Annex to the Communication from the Commission to the European Parliament, the European Council and the Council." https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/COM_2018_690_EN_annexe_autre_act_final1.pdf. Accessed: October 3, 2018.

85 | The CCP engages in extensive "party-to-party diplomacy" via its International Liaison Department and in some cases its United Front Department. Recently, this has expanded/deepen its contacts with various European right-wing parties. Examples include the AfD in Germany or the Five Star Movement (5SM) in Italy, see: Poggetti, Lucrezia (2018). "Italy Charts Risky Course With China-Friendly Policy." MERICS. October 11, 2018. https://www.merics.org/cn/node/8256. Accessed: October 11, 2018; Benner, Thorsten et. al. (2018). "Authoritarian Advance: Responding to China's Growing Political Influence in Europe." GPPi [The Global Public Policy Institute]. February 5. https://www.gppi.net/2018/02/05/authoritarian-advance-responding-to-chinas-growing-political-influence-in-europe. Accessed: October 18, 2018.

86 | There are over forty cities that have been selected to test various new measures. In addition, Beijing and other large cities have also introduced measures for individual credit ratings. See: Ohlberg, Mareike, Shazeda, Ahmed and Lang, Bertram (2017). "Central Planning, Local Experiment – The Complex Implementation of China's Social Credit System." MERICS. December 12. https://www.merics.org/sites/default/files/2017-12/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf. Accessed: October 5, 2018; Bloomberg (2018). "Beijing to Judge Every Resident Based on Behavior by End of 2020." November 21. https://www.bloomberg.com/news/articles/2018-11-21/beijing-to-judge-every-resident-based-on-behavior-by-end-of-2020. Accessed: November 22, 2018.

[87] Two examples are an attempt to force global airlines to adopt China's preferred terminology to refer to Taiwan by threatening, among other things, to hold them accountable under "Civil Aviation Industry Credit Management Measures (Trial Measures)" (see Hoffmann, Samantha (2018). "Technology-Enhanced Authoritarian Control With Global Consequences." Australian Strategic Policy Institute. June 28. https://www.aspi.org.au/report/social-credit. Accessed: September 28, 2018.) and the attempt to include political criteria in a social credit related assessment scheme for German NGOs in China (Giesen, Christoph and Strittmatter, Kai (2018). "Wie Peking deutsche Stiftungen drangsaliert." [How Beijing bullies German foundations] Süddeutsche Zeitung. July 9. https://www.sueddeutsche.de/politik/exklusiv-wie-china-deutsche-stiftungen-drangsaliert-1.4045372. Accessed: October 3, 2018).

[88] One example is the System Risk Indication (SyRI) program used in parts of the Netherlands that uses big data analytics to identify individuals supposedly abusing the welfare state. While the overall legal framework to challenge the system and potential abuse are better in Europe, this is quite close to how the Chinese government thinks about social credit, see Well, Louisa (2018). "High-Risk Citizens". Algorithm Watch." July 4. https://algorithmwatch.org/en/high-risk-citizens/. Accessed: September 24, 2018. Another example is Germany's Schufa, which uses an intransparent algorithm to assess people's financial creditworthiness, see Algorithm Watch (2018). "OpenSCHUFA – Shedding Light on Germany's Opaque Credit Scoring." February 21. https://algorithmwatch.org/en/openschufa-shedding-light-on-germanys-opaque-credit-scoring/. Accessed: September 24, 2018.

Contributors

Kristin Shi-Kupfer, Director of the Research Area on Public Policy and Society, heads MERICS' research on politics, society and the media. She is an expert on China's digital politics, ideology, media policy, civil society and human rights. She previously worked as a research associate at the University of Freiburg's Institute for Sinology. She earned her PhD from Ruhr University Bochum with a thesis on spiritual and religious groups in China after 1978. From 2007 to 2011, she was the China correspondent for several German media. Shi-Kupfer is a member of the expert committee of the German-Chinese platform on innovation under the Federal Ministry of Education and Research.

Mareike Ohlberg, Research Associate, focuses on China's subnational politics, official media policy as well as developments in Hong Kong and Taiwan. Ohlberg holds a PhD in Chinese Studies from the University of Heidelberg and an MA from Columbia University. In her thesis, she analyzed changes in China's global propaganda outreach since 1978. Prior to joining MERICS, Ohlberg spent a year as an An Wang Postdoctoral Fellow at the Fairbank Center for Chinese Studies at Harvard University and another year as a postdoctoral researcher at the Cheng Shewo Institute for Chinese Journalism at Shih Hsin University in Taipei.

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, Head of Publications, MERICS
Mary Hennock, Freelance Editor

Design
STOCKMAR+WALTER Kommunikationsdesign

Layout and Graphics
Alexandra Hinrichs, Graphic Designer, MERICS
Titlegraphic: Wu Yimeng (Studio Wu)

Printed in Berlin, Germany

ISSN (Print): 2509-4319
ISSN (Online): 2509-5862

www.merics.org