Wilfried
Martens Centre
for European Studies

Made in China

Tackling Digital Authoritarianism

Dimitar Lilkov

Wilfried
Martens Centre
for European Studies

Made in China

Tackling Digital Authoritarianism

Dimitar Lilkov

Credits

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE 1000

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

For more information please visit www.martenscentre.eu.

External editing: Communicative English bvba
Layout and cover design: Gëzim Lezha,
Visual Communications Assistant, Martens Centre
Typesetting: Victoria Agency
Printed in Belgium by Puntgaaf, Kortrijk

This publication receives funding from the European Parliament.

Contents

About the Martens Centre — **04**

About the author and acknowledgements — **06**

Executive summary — **08**

China: opening a new chapter — **10**

A blueprint for digital authoritarianism — **16**

- Setting the scene — 17
- Cyber sovereignty — 20
- Techno-nationalism — 22
- Made in China 2025 — 24
- Mass surveillance — 26

Raising the stakes: the Chinese Social Credit System — **32**

- Personal scoring by private companies — 34
- National implementation: the joint punishment system — 38
- Local Social Credit pilots and public opinion — 40
- Social Credit and businesses: implications for European companies — 41
- The Chinese Social Credit System: a recap — 44

Exporting oppression: the global spread of digital authoritarianism — **46**

- The Belt and Road Initiative and its digital grip — 47
- Safe cities and surveillance technology — 50
- Implications for the EU — 56

Discussion and key takeaways — **60**

Policy recommendations — **66**

Bibliography — **70**

Keywords EU – China – Digital authoritarianism – Internet – Cyber independence – Social Credit System – Belt and Road – Surveillance – Xi Jinping

About the Martens Centre

The Wilfried Martens Centre for European Studies, established in 2007, is the political foundation and think tank of the European People's Party (EPP). The Martens Centre embodies a pan-European mindset, promoting Christian Democrat, conservative and like-minded political values. It serves as a framework for national political foundations linked to member parties of the EPP. It currently has 31 member foundations and two permanent guest foundations in 25 EU and non-EU countries. The Martens Centre takes part in the preparation of EPP programmes and policy documents. It organises seminars and training on EU policies and on the process of European integration.

The Martens Centre also contributes to formulating EU and national public policies. It produces research studies and books, policy briefs and the twice-yearly *European View* journal. Its research activities are divided into six clusters: party structures and EU institutions, economic and social policies, EU foreign policy, environment and energy, values and religion, and new societal challenges. Through its papers, conferences, authors' dinners and website, the Martens Centre offers a platform for discussion among experts, politicians, policymakers and the European public.

About the author and acknowledgments

Dimitar Lilkov is a Research Officer at the Wilfried Martens Centre, where he is responsible for matters involving the digital economy, energy and the environment. Dimitar is the host of the Martens Centre's 'Brussels Bytes' podcast series on technology and European policy. He has a master's degree in politics and government in the EU from the London School of Economics and a BA in international relations. Currently, he is pursuing a Ph.D. at the European studies department of Sofia University.

The author wishes to extend his gratitude to several colleagues and experts who have provided constructive support for the completion of this research paper. I would like to thank Jana Mišić for her research assistance and engaging discussions on surveillance technology. Special thanks to Roland Freudenstein for his insights and valuable feedback on the different sections, as well as to Tomi Huhtanen for his encouragement to tackle this complex topic. I also wish to express my appreciation to several other people who have made important suggestions on the overall text. Thank you for taking the time to share your expertise.

Specific parts of this paper would not have been possible without the valuable research and academic insights of a community of Sinologists and experts who have devoted their careers to understanding Chinese politics, law, media and culture. I would like to personally thank Jeremy Daum, Samantha Hoffman, Rogier Creemers and Mareike Ohlberg for their research endeavours and invaluable work on lifting the veil of the Chinese Social Credit System. The paper has also benefited from important insights garnered from independent projects such as China Law Translate and organisations such as the Mercator Institute for China Studies, the Australian Stategic Policy Institute and the Centre for Strategic and International Studies, among others.

Executive summary

Technology and breakthrough innovation have become central pillars in President Xi Jinping's vision for restoring China's leadership on the global stage. Economic advancement and the success of Chinese products internationally, however, are only part of Xi's ambitions. With the help of technology, the People's Republic of China has effectively institutionalised the mass monitoring, profiling and punishment of its citizens, taking these controls to unparalleled heights. These efforts are the culmination of a decades-long strategy to ensure the undisputed rule of the Chinese Communist Party and to exert massive societal control in order to prevent political dissent. By advocating the importance of cyber sovereignty China is challenging the current framework of Internet governance. The country is implementing a new model which restricts online privacy and free expression by default and pushes economic entities to cooperate in sharing sensitive personal information and vital data with the government.

In parallel, China is pursuing an aggressive agenda of techno-nationalism which aims to move the country closer to technological self-sufficiency and to maximise the penetration of its technological giants in its internal market and on the global stage. These digital companies have been nurtured by generous public subsidies and successfully shielded from international competition while also being fed huge amounts of user data. Lastly, the government is increasing its efforts for the mass surveillance of Chinese citizens, including the reporting of daily activities and behavioural patterns. Such a comprehensive strategy is nothing less than a complex model of digital authoritarianism which utilises the resources of the whole state apparatus and imbues advanced technologies with Leninist and Maoist features for societal management and control.

The Chinese Social Credit System is a further expansion of the government's grip on its citizens. Still under construction, this is an integrated administrative tool for the evaluation and sanctioning of individuals, public institutions and private entities throughout the country. Though still far from a fully functioning digital instrument, the Social Credit System is likely to become one of the main mechanisms for political social management and for nudging Chinese individuals into 'trustworthy' behaviour. The system is expanding its application and is likely to impact the operations of domestic companies and also international private businesses operating in China. The arbitrary application of such corporate monitoring could discriminate against European companies and put them at a disadvantage in the foreseeable future.

The international aspect of Chinese digital authoritarianism is key in this analysis. China's oppressive model is no longer just applied domestically but is successfully being exported to other countries across different continents. Through its Belt and Road Initiative and separate economic partnerships, Beijing is rolling out technological infrastructure, data centres, fibre-optic cables and telecommunications networks—essentially building the digital backbone of these states. Such generous partnerships are sealed with the help of Chinese loans which guarantee Beijing's growing political influence and long-term dependence on Chinese technological products, support and maintenance. In addition, China is also influencing countries in Asia and Africa, encouraging them to adopt its own vision for Internet governance and legislation, while Chinese companies are supplying them with advanced surveillance technology which can be directly abused by authoritarian governments. Last but not least, Chinese exports of technological equipment and software, even to EU member states, raise serious cybersecurity concerns and propel fears about China's increased involvement in cyber-espionage and cyber attacks.

This research paper analyses the unique features of the Chinese model of digital authoritarianism and its international spillovers. The paper further examines the impact of China's digital rise on global affairs and the consequences for EU member states. A comprehensive European strategy is needed to withstand the direct threat to the EU's vital interests and inherent democratic values. Ultimately, Europe also needs to evaluate its own relationship with third-country technology companies and the exploitation of personal data, as well as the related risks of behavioural profiling and citizen surveillance.

The EU must make sure that its citizens have the necessary institutional and legal protection from abuses of modern technology such as facial-recognition software or the advanced application of artificial intelligence. The EU should remain a global influence when it comes to a human-centric regulatory approach to technology, and stand ready to oppose the spread of digital authoritarianism. Additionally, the Union has to strengthen its own digital single market and ensure that it remains a global player in developing cutting-edge technology and breakthrough innovation. On the individual level, European citizens must be aware of the risks stemming from their own daily exposure to foreign digital companies and third-country social media platforms which have been granted a startling degree of access to their private lives.

China: opening a new chapter

In recent years, the People's Republic of China has managed to capture the minds of politicians and pundits alike. Lifting more than 600 million people out of poverty in three decades and putting Chinese gross domestic product (GDP) among the world`s top economies remain undeniable feats. The economic centre of the world is shifting from the Atlantic to Asia and China has played no small part in this. However, the Chinese success story remains a dubious tale. Progress has been achieved within a state which keeps an authoritarian grip on its internal political system and which continues to blur the lines between public and private enterprise. Domestic companies in China still receive significant amounts of state subsidies annually and the higher echelons of the Communist Party are able to exert pressure on the operations and management of many private businesses. Most worryingly, 30 years after the Tiananmen massacre, China continues to blatantly disregard some of the basic human rights of its citizens.

On the international level, the Asian hegemon is a force to be reckoned with. From trade disputes in negotiation chambers with Western counterparts to actual physical skirmishes on the streets of Hong Kong, one cannot escape the sense that frictions are growing. The latest Sino-American trade rift might appear to be a breaking point, but Beijing has a long-standing history of confrontation with both the US and the EU. By denying foreign companies access to its internal market, China has systemically pursued an unbalanced and unequal economic relationship with the EU. The forced technology transfer practices of the Chinese government have compelled numerous European firms to undermine their intellectual property rights and share their technology with Chinese companies. Cyberwarfare by state proxies and the clandestine engagement of Beijing with global disinformation efforts are further exacerbating tensions.

Emboldened by its economic stature and eyeing the potential of exploiting other countries' vulnerabilities, China has opened a new chapter in its act on the international stage, one of potential confrontation and open questioning of the established rules on industrial policy, global development and Internet governance. This is a phase of expansion through economic influence and the aggressive exportation of domestic goods and technology. Such a change also marks a shift in the general direction of Chinese foreign policy, which has traditionally been aimed at keeping a low profile in international affairs.

This research paper endeavours to analyse the People's Republic of China's recent digital rise and its long-term implications for the EU and global affairs. The paper posits that the current Chinese strategy for digital governance and technological advancement serves at least two main purposes. First, the Chinese model of cyber sovereignty and techno-nationalism is an essential component in ensuring the long-term political control of the Communist Party of China (CPC). Xi Jinping's vision harnesses the opportunities provided by online censorship, mass surveillance, digital profiling and artificial intelligence (AI) with the aim of establishing complete societal control under the pretence of trust and security. An additional concern is the integration of Chinese technological giants into this complex architecture which aims to oppress political dissent and effectively shape public discourse.

Second, Beijing is pursuing the strategic goal of ensuring its global technological leadership in order to guarantee its political and economic advantage in the long run. It aims to fund and supply the mass roll-out of technological infrastructure in a number of developing countries worldwide, ensuring their dependency on Chinese technological support. In parallel, China is also pushing many of these countries to adopt its approach to Internet restrictions, mass surveillance and limitations on civil liberties. Worse still, Chinese companies are becoming the biggest exporters of cutting-edge AI surveillance technology globally, which is already having negative implications for a number of countries with authoritarian governments and poor human rights track records. Essentially, China is pursuing a path of digital authoritarianism which has implications beyond its own borders.

These developments are raising substantial concerns in many European capitals. The European Commission recently described China as an important cooperation and negotiation partner in a number of areas but also as 'an economic competitor in the pursuit of technological leadership, and a systemic rival promoting alternative models of governance'.[1] The EU has de facto recognised that China has become a global actor with increasing aspirations in the international arena. Beijing's influence is rising and is challenging not only European economic objectives but also the EU's long-term interests and fundamental democratic values. For Europe, China's digital authoritarianism is a growing threat and its overall model of governance, a systemic rival.

[1] European Commission, *EU–China—A Strategic Outlook*, Communication, JOIN (2019) 5 final (12 March 2019).

A blueprint for digital authoritarianism

Setting the scene

In 2012 Mr Xi Jinping became General Secretary of the Central Committee of the Communist Party of China and the country's president. In 2018 the National People's Congress rubber-stamped the official removal of the two-term limit on the presidency and opened up the possibility of Xi Jinping remaining in power for life. The previous form of attempted collective leadership was snubbed; the current power structure of the presidency can only be compared with the chairmanship of Mao Zedong. This *déjà vu* became stronger when 'Xi Jinping Thought' became part of the Chinese constitution and an object of study nationwide as a central tenet of the country's political ideology. These 'thoughts' touch upon socialist values and the state's reforms, and offer an overall policy outline for the future development of the CPC and China itself.

Going beyond bureaucratic jargon or a Communist utopia, there is at least one additional thought that is central to Xi's long-term vision for China—the importance of the Internet and modern technology. The new Chinese president has expanded on the patchy initial steps taken by his predecessors and has made cyber policy a key governmental priority. Under Xi's auspices the Cyberspace Administration of China was established in 2014 with the role of regulating and censoring online content and providing oversight functions. This structure is directly accountable to the Central Cyberspace Commission, which is headed by Xi himself. In 2018, after internal reorganisations, both structures were given a boost[2] in terms of resources and political clout and are now among the leading administrative champions in China's intricate governance framework. Under Xi's reign China has adopted its first cybersecurity law and introduced stringent instruments for policing the Internet. Heavy demands are placed on Internet companies, which have to constantly survey their networks and submit information to the state authorities on request.[3]

A state news agency has reported that two million Chinese are employed to keep track of online discussions and to monitor microblogs.[4] The staggering number of people might be consciously overblown

[2] R. Creemers et al., 'China's Cyberspace Authorities Set to Gain Clout in Reorganization', *New America*, 26 March 2018.
[3] X. Quiang, 'The Road to Digital Unfreedom: President Xi's Surveillance State', *Journal of Democracy* 30/1 (2019), 55.
[4] *BBC News*, 'China Employs Two Million Microblog Monitors State Media Say', 4 October 2013.

by the state to propel fear and ensure online discipline, but in the last several years officials have made sure that online political dissent or attempts to organise protest rallies have not gone unnoticed. Nor do the Chinese authorities shy away from actively intervening and directing online conversations. A large-scale study[5] estimated that the government fabricates and posts close to 450 million social media comments a year. In parallel, liberal voices are very rarely admitted on Chinese social media, with official party–state narratives dominating Internet debates.[6] The combination of draconian online censorship and the generation of orchestrated website/social media content means that the authorities play a huge role in shaping popular opinion online.

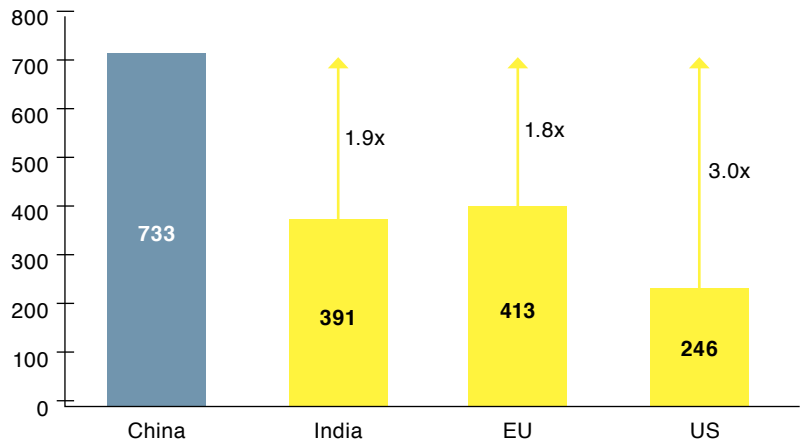
These policies were not developed in a vacuum. Xi's predecessors laid down some essential elements for constructing the Chinese version of the web. The 'Golden Shield' (infamously known as the Great Firewall of China), which can block IP addresses and domain names, was developed in the early 2000s. Scrutiny of website comments and the tracking down of dissidents who voice their concerns online also predate the current president by at least a decade. However, only after Xi Jinping rose to power did China place so much emphasis on Internet governance and establishing a comprehensive administrative system to keep all aspects of online life in check. In the words of Lu Wei, the former director of China's State Internet Information Office, the country's Internet has developed at a fierce pace but it needs to 'have brakes, just like a car'.[7] Not surprisingly, China is reported to be the world's worst abuser of Internet freedom.

As the country is on track to reach 800 million Internet[8] users in the near future (Figure 1), almost a quarter of all users globally, the Internet has gained major importance for Chinese politics and business development. It is interesting to note that almost all of the Internet users in China are also mobile users. This is a huge achievement in terms of personal convenience, access to services and optimising communication for the majority of the population. However, for Chinese officials access to the mobile Internet is not only a tool for economic growth, but also an effective instrument for social management

[5] G. King et al., 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', *American Political Science Review* 111/3 (2017), 484–501.
[6] K. Shi-Kupfer and M. Ohlberg, 'The Party Does Not Yet Rule Over Everything', Mercator Institute for China Studies (29 November 2018).
[7] D. Bandurski, 'Lu Wei: The Internet Must Have Brakes', *China Media Monitor* (11 September 2014).
[8] E. Charlton, 'Most People on the Internet Live in This Country', World Economic Forum (27 June 2019).

and ensuring absolute control across the vast provinces of the country. Until recently online privacy was an unfamiliar concept in China. Now, however, the Chinese are increasing their demands for additional privacy safeguards, although these demands are mostly to protect against the intrusions of technology companies. There have been several challenges[9] to Chinese Internet giants regarding personal data privacy, but the matter of the personal data relationship between consumers and the state is a completely different story. Various pieces of national legislation in China give the government exclusive powers to access private-sector data on the grounds of state and public security. If the state wants to acquire specific personal data from Internet providers or lines of correspondence between users on Chinese social media, there is little to prevent this.

Figure 1 Number of Chinese Internet users compared to other major economies (in millions of persons)



Source: IMF, 'People's Republic of China', IMF Country Report no. 18/240 (July 2018).

[9] W. M. Wenyan, 'China Is Waking up to Data Protection and Privacy. Here's Why That Matters', World Economic Forum (12 November 2019).

Cyber sovereignty

Beijing's objections to the way the Internet operates stem from the dominant role the US has played in the web's technical and organisational architecture since its inception. The Asian country wants to challenge the bottom-up model of Internet governance which, in China's view, is dominated by Western companies and civil society organisations.[10] The Internet Corporation for Assigned Names and Numbers, for example, is a California-based non-profit entity which provides an important bedrock for the Internet's structural design. Organisations such as it have pioneered the multi-stakeholder model in which leaders from civil society, private companies and government collectively determine the rules of Internet operation.[11] China sees this as an affront to the role of national jurisdictions. If the US and its allies regard the multi-stakeholder approach as most appropriate, China believes in a multilateral one in which national governments have a greater say in the global governance of the web.[12] This clash of visions has been a feature at numerous international fora on telecommunications and cyber governance since the 2000s. Countries such as Russia, Saudi Arabia, Algeria and Sudan have supported[13] China's previous international efforts to reinforce the sovereign grip on Internet governance. In recent years Beijing has decided to play a more active role by setting up the annual World Internet Conference in Wuzhen, China. At the 2015 forum Xi Jinping urged the world to respect each country's cyber sovereignty and observed that the current rules governing cyberspace 'hardly reflect the desires and interests of the majority of countries'.[14] The Chinese president is openly pursuing a path of 'cyber sovereignty'—wherein individual nations should be able to manage and restrict the web within their borders.

China's additional concerns with the traditional architecture of the web are twofold. First, open access to information and unfiltered debate are a direct threat to the reign of the CPC. Online users in China

[10] A. Segal, 'When China Rules the Web', *Foreign Affairs*, September/October 2018.
[11] M. Kolton, 'Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence', *The Cyber Defence Review* 2/1 (2017), 121.
[12] For a comprehensive discussion on the difference between the two and Beijing's overall philosophy for cyber sovereignty, see L. Wei, 'Cyber Sovereignty Must Rule Global Internet', *Huffpost*, 15 December 2014.
[13] J. Masters, 'What Is Internet Governance?', Council on Foreign Relations (23 April 2014).
[14] *China Daily Asia*, 'Xi Slams "Double Standards" in Cyberspace', 16 December 2015.

have used the web to voice criticisms of the party and the growing levels of corruption, or to share relevant information on current events. State leaders fear the potential of the Internet to bring together thousands of people and organise protests which are beyond governmental control. The second major concern for China is external interference. In the aftermath of the Edward Snowden whistle-blower leaks of 2013, Beijing became extremely anxious about the US intelligence community's capacity to access web networks and carry out cyber-espionage. Additional WikiLeaks files suggested that the US National Security Agency tapped high-level phone calls, even involving German Chancellor Angela Merkel. The Snowden revelations added fuel to Beijing's fears that the US was using its privileged position in the cyber domain to guarantee its future hegemony.[15] The CPC leadership and Xi himself became convinced of the growing need to ensure independent networks and reinforced mechanisms for state intervention.

The doctrine of cyber sovereignty can be seen as an ominous milestone for global affairs. It is an overt attempt to introduce a new model of Internet governance which directly opposes the current global framework of the free and open web. It is also China's rallying call to other countries across the globe that share its vision and that are also sceptical of the Western-led vision of Internet freedom. The Russian Federation has followed in China's footsteps with the introduction of a new law[16] aiming to establish its own 'independent' Internet and increase domestic censorship. Vietnam has also recently adopted a cybersecurity law[17] that mirrors China's legislation, and several other neighbouring or former Soviet Union countries are aspiring to copy Beijing's 'best practices' in the domain of cyber independence too. But this vision may not remain limited to Asia. Many states in the developing world have a digital disadvantage and have yet to build telecoms infrastructure in their fragile economies. China increasingly provides network infrastructure and software support[18] in many such states and might draw them in as allies in its vision for online governance.[19]

[15] N. Inskter, *China's Cyber Power* (London: Routledge, 1st edition), 72.
[16] N. Hodge and M. Ilyshina, 'Putin Signs Law to Create an Independent Russian Internet', *CNN*, 1 May 2019.
[17] J. Hookway, 'Vietnam Tightens Grip on Internet With Data-Storage Law', *The Wall Street Journa*l, 12 June 2018.
[18] Inskter, *China's Cyber Power*, 10.
[19] The international aspect of China's digital authoritarianism is analysed in more detail in the closing sections of this paper.

Techno-nationalism

Promoting an alternative cyber-reality requires more than online censorship and strict legislation. It demands a substantial cut-off from foreign digital platforms providing unfiltered services in China, as well as increased independence from Western suppliers of hardware and communications equipment. To achieve these aims, China has actively pursued a unique brand of techno-nationalism.

When it comes to limiting foreign competition, China is a global front-runner. The total ban on high-ranking popular websites/social media platforms such as Google, Wikipedia, YouTube and Facebook in mainland China is standard practice. But that is just the tip of the iceberg. The Cyber Administration of China is constantly expanding the list of banned websites and more than three thousand[20] were shut down or had their foreign website licences revoked in 2018. Those which do operate in China have to abide by the stringent cybersecurity law which recently entered into force. This piece of legislation affects all networks and information systems in China with no exceptions for foreign-owned companies; it also aims to prevent any attempt to establish encrypted communications, virtual private networks or anonymous online accounts. All companies are required to supply sensitive information to the authorities on request. Most worryingly, certain types of information, including personal data, have to be kept at data centres in China.[21]

The ban on Google, Facebook and other major Silicon Valley tech companies does not mean that Chinese users suffer from the absence of similar digital products. They are simply replaced by home-grown versions which provide search (Baidu), entertainment (Tencent), e-commerce (Alibaba), social media (Weibo) and text messaging (WeChat) services. By banning foreign competition, China has strategically nurtured its own tech champions and also encouraged them to expand internationally. China's huge domestic market and lax privacy rules gave these tech behemoths almost unlimited access to user data in the past, enabling them to optimise their services and improve machine-learning algorithms. Many of these companies were not only developed in a competition-free environment but were also given preferential access to government funding

[20] L. Yuan, 'A Generation Grows up in China Without Google, Facebook or Twitter', *The New York Times*, 6 August 2018.
[21] S. Wong and M. Martina, 'China Adopts Cyber Security Law in Face of Overseas Opposition', *Reuters*, 7 November 2016.

for years on end. Chinese domestic subsidies for national companies have become globally infamous. A lack of transparency and the misreporting of official data have made pinpointing the exact amounts extremely difficult, but fiscal subsidies from the Chinese budget remain enormous.[22] The IMF estimates[23] that implicit support (i.e. land, credit and natural resources) for state-owned companies is hovering at around 3% of Chinese GDP, while in 2018 China paid at least $22 billion in record corporate subsidies to domestically listed companies.[24] The recent rise of Chinese companies in sectors such as AI or blockchain is due, in part, to Chinese government support.[25] Protectionist domestic legislation also offers a layer of protection. The US Chamber of Commerce has found that the Chinese anti-monopoly law promotes industrial policy goals and boosts national champions through discrimination and protectionism.[26] The Chinese strategy has borne fruit. Four of the top 10 publicly traded Internet-based companies in the world in 2018 were Chinese.

The state's involvement does not stop there. Internal influence and pressure from the CPC are not only present but also growing substantially in the private sector. Media reports claim that party organisations and branches exist in 70% of the privately owned companies in China.[27] Many of China's tech giants, regardless of their ownership structure, remain far from independent. A recent in-depth study of the biggest Chinese tech companies found that around 200 party branches exist within Alibaba, 89 in Tencent and more than 300 in Huawei.[28] Research into the opaque ownership structures of some of these companies calls into serious doubt their status as private entities that are separate from the state.[29] Regardless of their success, many of China's tech giants remain domestic monopolies that are deeply enmeshed in the CPC's party line and state funding. More worryingly, this modus operandi has also spilled over into the rest of the tech sector, impacting large and small companies. This intricate web involves many private players, state institutions and even the military. As succinctly summed up by the Mercator Institute for China Studies: 'It would be hard-to-impossible to track the web of party influence, state control mechanisms and international linkages that

[22] S. Kennedy and D. Rosen, 'Market Metrics: A Fact-Based Approach to the Chinese Economic Challenge', Center for Strategic and International Studies (10 October 2019).
[23] IMF, 'People's Republic of China', Country Report no. 19/274 (August 2019), 37.
[24] T. Hancock and J. Yizhen, 'China Pays Record $22bn in Corporate Subsidies in 2018', *Financial Times*, 27 May 2019.
[25] US–China Economic and Security Review Commission, *2017 Annual Report to Congress* (2017), 526.
[26] US Chamber of Commerce, 'Competing Interests in China's Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy' (9 August 2014), 1.
[27] M. Martina, 'Exclusive: In China, the Party's Push for Influence Inside Foreign Firms Stirs Fears', *Reuters*, 24 August 2017.
[28] D. Cave et al., *Mapping China's Tech Giants*, Australian Strategic Policy Institute (18 April 2019), 7.
[29] C. Balding and D. Clarke, *Who Owns Huawei?*, SSRN Scholarly Paper (17 April 2019).

surrounds China's sprawling ecosystem of innovative start-ups, venture capital funds, local governments—and the military'.[30]

Made in China 2025

The second objective of pursuing a techno-nationalist strategic agenda is to reduce dependence on foreign imports of vital digital and communications hardware. This objective does not stem solely from cybersecurity or military concerns. China is extremely dependent on foreign imports of digital equipment for developing its own technological products. The US is one of the key exporters of microchips and tech equipment to China. In 2018 the US briefly banned American firms from selling parts to ZTE, China's second biggest telecoms company. US exports provide close to 30% of the components used in ZTE's equipment and the ban precipitated a crisis, as well as substantial financial losses for the company, before it was lifted.[31] This served as one of the many wake-up calls for Chinese decision-makers, who have developed a comprehensive strategy to ensure long-term technological self-sufficiency.

Made in China 2025 is an ambitious effort to propel the Chinese economy from low-value-added manufacturing of cheap consumer goods to a high-tech economy with an upgraded domestic industry. The aim is to achieve this goal by prioritising 10 strategic sectors and employing a wide-ranging toolbox which includes, among other things, massive state funding, increased research and development (R&D) spending, China-specific standards and the development of specialised talent.[32] In 2018, China spent more than 2% of its GDP, or close to $300 billion, on R&D.[33] Targeted research funding is allocated to strategic sectors such as semiconductor optimisation, telecommunications technology, quantum computing and AI. It is reported that China has spent 10 times more on quantum R&D than the US and that the Asian state is also taking the lead when

[30] K. Shi-Kupfer and M. Ohlberg, *China's Digital Rise: Challenges for Europe*, Papers on China no. 7, Mercator Institute for China Studies (April 2019), 9.
[31] S. Stecklow et al., 'U.S. Ban on Sales to China's ZTE Opens Fresh Front as Tensions Escalate', *Reuters*, 16 April 2018.
[32] K. Koleski and N. Salidjanova, *China's Technonationalism Toolbox: A Primer*, US–China Economic and Security Review Commission (28 March 2018), 1.
[33] M. J. Zenglein and A. Holzmann, *Evolving Made in China 2025*, Papers on China no. 8, Mercator Institute for China Studies (July 2019), 11.

it comes to filing patents.[34] The country is also demonstrating a growing ambition to become a global player in producing pioneering AI technology. There is an ongoing debate as to whether China will soon outpace the US when it comes to AI funding, academic research and its talent pool of highly skilled experts. In its usual style, China has announced that it intends to become the world leader in AI by 2030, with the aim of making the industry worth 1 trillion yuan (close to $150 billion).[35]

An additional key aim of the Made in China strategy is reversing China's dependence on other countries for essential components. Beijing's goal is to produce 40% of the semiconductors vital for technological development by 2020 and 70% by 2025.[36] This is to be accomplished by a combination of massive government funding, the expansion of foreign investment and the acquisition of non-domestic businesses. Achieving the overall goals of Made in China 2025 will require continuous reliance on governmental financial subsidies, preferential loans, tax breaks and other direct/indirect aid, the total of which is difficult to estimate but is projected to be in the hundreds of billions of dollars.[37]

All of these efforts would also help to overcome the potential stagnation of the Chinese economy after a period of stellar economic growth. Many other developing countries have been plagued by the 'middle income trap, which leaves them stuck at the same level of economic development after reaping the benefits of cheap labour, urbanisation and industrialisation. Chinese policymakers want to push the country towards higher-value services and revamped industry. In essence, Made in China 2025 can be seen as copying similar efforts elsewhere, such as Germany's 'Industry 4.0' agenda. The difference between the Chinese strategy and others is its commitment to also guarantee its independence in key technological and industrial sectors—Beijing not only wants to catch up with Western economies but also to displace their industrial leadership. Xi Jinping has embraced Made in China 2025 as a signature project and has officially shared his vision for turning China into the world's manufacturing and technological superpower. One might conclude that the current Chinese strategy pursues only absolute economic advantages and disregards comparative ones: it is as if today's policymakers have only read Adam Smith and snubbed David Ricardo.[38]

---

[34] Shi-Kupfer and Ohlberg, *China's Digital Rise*, 32.
[35] A. Kharpal, 'China Wants To Be a $150 Billion World Leader in AI in Less Than 15 Years', *CNBC*, 21 July 2019.
[36] J. A. Lewis, 'China's Pursuit of Semiconductor Independence', Center for Strategic and International Studies (January 2019), 2.
[37] J. McBride and A. Chatzky, 'Is "Made in China 2025" a Threat to Global Trade?', Council on Foreign Relations (2019).
[38] Adapted from R. Atkinson, speech made at a discussion on 'The Role of Technology in the US–China Trade War', organised by the Brookings Institution, Washington, DC, 18 July 2019.

It remains to be seen whether China manages to successfully implement such an ambitious restructuring of its industry. Spending huge amounts of state funding cannot guarantee positive outcomes, especially in endeavours such as reaching technological self-sufficiency—a goal which China has consistently failed to achieve in the past decade. Many Chinese manufacturing and technology sectors remain vulnerable and are suffering from the inherent flaws of a socialist market economy where central planning takes precedence. China is making undeniable economic and technological progress, but one must remain wary of the frequently disseminated narrative of China's inevitable technological dominance in years to come—a tale which Beijing is only too happy to support.

Mass surveillance

The final element of the Chinese blueprint for digital authoritarianism is mass surveillance. Claiming that China is a surveillance state would be an understatement. China is *the* surveillance state. Eight out of the 10 most monitored cities in the world are in China.[39] Close to 200 million cameras are installed within the country and the government plans to at least double (if not triple) this capacity by the end of 2020. China's ambitious policymakers have laid out plans to achieve full video coverage of key public areas, with the city of Beijing lauded as fully covered by constant video surveillance.[40] Given that China is investing ever-increasing funds in its domestic security, ubiquitous video surveillance may well become a fact of life in the 2020s in many of China's biggest cities. Sources estimate that in 2017 Chinese domestic security spending hit $197 billion, an even greater amount than was reportedly spent on the overall external defence of the country.[41]

The new generation of surveillance tech used in China allows smart connectivity between devices, establishing an all-encompassing network which can follow individuals through crowds and traffic. All of this data is integrated into a comprehensive video-surveillance system depressingly named 'Skynet'.

[39] P. Bischoff, 'The World's Most-Surveilled Cities', *Comparitech* (15 August 2019).
[40] A. Mitchell and L. Diamond, 'China's Surveillance State Should Scare Everyone', *The Atlantic*, 2 February 2018.
[41] A. Zenz, *China's Domestic Security Spending: An Analysis of Available Data*, The Jamestown Foundation, China Brief 18/4 (12 March 2018).

The system was set up more than a decade ago and has recently been completed, making it the largest and most sophisticated video-surveillance network in the world, with the ability to cross-check data from cameras all over China.[42] More advanced surveillance equipment can even recognise a person's height, gender and gait. The technological potential of the system was publicly demonstrated in 2017 when a BBC News correspondent volunteered to test its capacity—it took only seven minutes for the surveillance system to pinpoint his location based on the integrated facial-recognition surveillance software.[43] One can but be amazed at the vast array of tracking equipment—devices include not only smart cameras, but portable facial-recognition glasses, voice-recognition software to trace phone calls and even hi-tech surveillance drones which purposely resemble birds in order to avoid suspicion. Chinese policemen sometimes even request that the mobile phones of random passers-by are handed over for an inspection of recent activity and the applications installed on the device. In late 2019, the Chinese authorities made it obligatory for citizens to scan their faces when registering for new mobile phone services.[44]

The Chinese surveillance arsenal does not stop there—public authorities have been compiling an extremely controversial DNA database which is intended to include 100 million records by 2020.[45] This massive database mostly features samples from foreign migrants or ethnic minorities and is an egregious violation of their human rights. In October 2018 the US blacklisted 28 Chinese companies and government entities[46] because of their direct involvement in the disgraceful treatment of the Muslim minority in Xinjiang (see Box 1). The blacklist includes Megvii, Yitu and SenseTime, which are China's national champions in developing facial-recognition software. These companies have seen an astronomical rise in terms of client base and market valuation—for example, Megvii has reportedly raised more than $1 billion from different investment funds and companies and was valued at $4 billion in 2019.[47]

[42] C. Rollet, 'China Public Video Surveillance Guide: From Skynet to Sharp Eyes', IPVM (14 June 2018).
[43] J. Liu and W. Xiqing, 'In Your Face: China's All-Seeing State', *BBC News*, 10 December 2017.
[44] *BBC News*, 'China Due to Introduce Face Scans for Mobile Users', 1 December 2019.
[45] W. Fan et al., 'China Snares Innocent and Guilty Alike to Build World's Biggest DNA Database', *The Wall Street Journa*l, 26 December 2017.
[46] US Bureau of Industry and Security Commerce, *Addition of Certain Entities to the Entity List*, Federal Register (10 September 2019).
[47] T. Simonite, 'Behind the Rise of China's Facial-Recognition Giants', *Wired*, 9 March 2019.

Box 1 Digital authoritarianism in action: the oppression of Uighurs and other minorities in Xinjiang

The Xinjiang Autonomous Region is the largest province in China and its population is comprised of numerous ethnic groups—the biggest is that of Uighur Muslims, followed by Han Chinese. Historically, ethnic tensions were exacerbated after the state-encouraged mass migration of Han Chinese to the region. In recent years there have been many instances of riots and physical attacks which have led to numerous deaths and injuries. In response, the Chinese authorities have started a massive crackdown on freedom there, mostly affecting Uighur Muslims and other minorities, which has reached dramatic heights. Between eight hundred thousand and two million Uighurs and other Muslims, such as Kazakhs and Uzbeks, are assumed to have been physically detained[48] without being charged of explicit crimes or public misdemeanours. A UN panel of human rights experts has evidence of a 'massive internment camp that is shrouded in secrecy'.[49] The detainees are separated from their families and incarcerated for various periods of time while suffering physical and psychological abuse.

Investigations by journalists have showcased the massive expansion of detention camps and the drastic increase in security and surveillance equipment throughout the region. Using the excuse of preventing religious extremism, authorities have instituted a draconian surveillance regime to track and profile most of the urban residents in Xinjiang. A specific grid-management system splits the villages and cities into closely monitored zones with omnipresent video surveillance and widespread police check-points. The authorities are also collecting photos, fingerprints and even DNA samples from minority groups to create a vast database, turning the region into a 'frontline laboratory for data-driven surveillance'.[50] The monitoring of social media conversations via WeChat has also led to arrests of Uighur Muslims, with ripple effects for their relatives and friends.

[48] L. Maizland, 'China's Repression of Uighurs in Xinjiang', Council on Foreign Relations (25 November 2019).
[49] S. Nebehay, 'U.N. Says It Has Credible Reports That China Holds Million Uighurs in Secret Camps', *Reuters*, 10 August 2018.
[50] Quiang, 'The Road to Digital Unfreedom', 57.

China initially denied the very existence of such measures or internment camps, but eventually described them as vocational and educational camps set up in the interest of helping their inmates. In essence, China aims to supress religious identities in the region and ensure the long-term assimilation of Uighur Muslims into the Han Chinese community. In July 2019 UN ambassadors from 22 states including Britain, Canada, France, Germany and Japan co-signed a letter objecting to China's continued oppression in Xinjiang.[51] In October 2019 the US imposed visa restrictions on Chinese officials believed to be responsible for or complicit in these detentions. A spokesperson from the Turkish Ministry for Foreign Affairs has bluntly stated that more than a million Uighurs 'incurring arbitrary arrests are subjected to torture and political brainwashing in internment camps and prisons'.[52] A large-scale collaboration between investigative journalists who have seen highly classified government documents has shed additional light on the detailed plans for the mass crackdown on Muslims in Xinjiang, the operation of the detention camps, and the chilling details of the surveillance technology employed to monitor and profile each individual.[53]

[51] Human Rights Watch, 'UN: Unprecedented Joint Call for China to End Xinjiang Abuses' (10 July 2019).

[52] Turkey, Ministry of Foreign Affairs, 'Statement of the Spokesperson of the Ministry of Foreign Affairs, Mr. Hami Aksoy', QA-6 (9 February 2019).

[53] B. Allen-Ebrahimian, 'Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm', China Cables, International Consortium of Investigative Journalists (24 November 2019).

Figure 2 The China model of Internet control

Source: A. Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (October 2018).

Raising the stakes: the Chinese Social Credit System

Even though China manages to monitor many of its citizens offline and online, the state is still far from having an efficient administration which can integrate all of the information from its different branches, agencies and courts in order to keep coordinated records on all of its 1.4 billion citizens. In the past, Chinese policymakers explored ideas for a gigantic database which would integrate all available record data on individuals from different bureaucracies with the aim of monitoring their behaviour and eventually punishing deviations. So far, such a concept has been too ambitious to achieve due to the lack of technological capacity and the complexity of ensuring the necessary coordination between the different parts of China's arcane administration. For most of the last decade, however, China has been working towards achieving exactly this goal.

In 2014 China rolled out its 'Planning Outline for the Construction of a Social Credit System (2014–2020)' as a key component of its socialist market economy and social governance system. Set up as an ambitious legal and regulatory framework, the broad document aspires to improve the trustworthiness of individuals, private organisations and public institutions. China has a long-standing problem with maintaining high levels of public trust within society—a problem that affects institutions and individuals alike. China's public bodies have faced problems when implementing national legislation or enforcing court judgments in some provinces. On an everyday level, there are numerous instances of petty fraud, bribery and financial scamming, which have plagued public trust in society. Historically, distrust among the Chinese population also stems from the atrocities of the Cultural Revolution and the deeds of the CPC itself between 1966 and 1976. The violent class struggle imposed by the authorities during this period led to the persecution or death of millions Chinese citizens. At the same time, the CPC also set up intricate state security networks for the monitoring and reporting of young people and intellectuals, as well as the administrative and academic elite.

With the advent of breakthrough technology and big data, the Chinese authorities realised that a comprehensive system for monitoring individual and organisational behaviour might ensure compliance and thus restore 'trust' within society. For the private sector, social credit is seen as a framework to enhance transparency and efficiency, as well as to ensure increased compliance with government regulations. On the individual level, such an integrated system is seen as a successful mechanism for ensuring lawful behaviour, maintaining social order and preserving the political status quo within the country. The Planning Outline recognises social credit as an important mechanism to 'commend

sincerity and punish insincerity'[54] within a 'harmonious' socialist society.

One quickly realises that such a system will not only be bound by the legality of individual or private company behaviour. The Social Credit System is intended to provide rewards or punishment based on not only the lawfulness, but also the morality of actions, covering the spectrum of economic, social and political conduct.[55] The ultimate arbiter of morality or proper conduct is, of course, the state and its governmental bodies. Essentially, the planned Social Credit System in China is a complex ecosystem for social management which is still in development and operates under the noble pretence of improving societal trust and legal compliance.

Personal scoring by private companies

The proposed Social Credit System has drawn increasing attention from Western media and public officials. Journalists' reports have described it as a dynamic personal three-digit score which can determine a person's place in society, or as an almost-comprehensive national system for monitoring personal behaviour. References to ominous sci-fi series, such as *Black Mirror*,[56] or George Orwell's dystopian *1984*[57] have been used as comparisons to convey the design and ultimate aims of the Social Credit System. US Vice-President Mike Pence has described it as 'an Orwellian system premised on controlling virtually every facet of human life'.[58] While most of these journalism pieces or political commentaries raise important concerns, these accounts have caused much confusion and contain many inaccuracies. Social Credit is a far more complicated system than is often described and some of

[54] People's Republic of China, 'State Council Notice Concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020)', GF No. (2014)21. For an unofficial English translation, see R. Creemers (ed.), 'Planning Outline for the Construction of a Social Credit System (2014-2020)', *China Copyright and Media: The Law and Policy of Media in China*, updated 25 April 2015.

[55] R. Creemers, *China's Social Credit System: An Evolving Practice of Control*, SSRN (9 May 2019), 2.

[56] P. Dockrill, 'China's Chilling "Social Credit System" Is Straight Out of Dystopian Sci-Fi, and It's Already Switched on', *Science Alert* (20 September 2018).

[57] A. Ash, '"1984" Algorithm to Control Life in China', *The Times*, 11 June 2017.

[58] The Hudson Institute, 'Remarks by Vice President Pence on the Administration's Policy Toward China' (4 October 2018).

the original media outlets that reported on these misperceptions have since tried to correct the record.[59] This confusion is natural due to the complexity of the topic, language barriers and the opacity of the Chinese system of governance.

The Chinese phrase 社会信用 can be translated as 'social credit' but can also be interpreted as 'public trust'. As previously noted, the authorities have justified the launch of the Planning Outline as a way of achieving the goal of restoring trust in Chinese society, which suffers from problems with enforcing court orders and various petty financial crimes. An additional feature for consideration is the fact that China continues to be at the top of the World Bank's ranking of countries for the number of adults who lack access to a bank account.[60] The country registers one of the lowest numbers of credit cards per person, as well. Because of this and the widespread use of cash in financial transactions, a huge chunk of Chinese society does not have a financial history or credit record, which has caused a substantial problem when it comes to loan applications.

To address this, in 2015 the People's Bank of China commissioned eight private companies to develop pilot schemes for credit reporting systems given that they possess large volumes of data from their growing user bases.[61] A prominent example of these pilots is Sesame (Zhima) Credit, developed by Ant Financial Services group, an affiliate of the e-commerce giant Alibaba. Sesame Credit is a private system which monitors its users' online purchases, loan payments, financial transfers and interactions with other users on its platform to provide a personal credit score between 350 and 900. A higher score unlocks access to personal perks such as easy forms of credit or deposit-free services for renting accommodation or transport. The higher the Sesame Credit score, the more reliable and financially secure the person is presumed to be. Participation in this private system is voluntary on an opt-in basis and has been developed in parallel to the other credit reporting systems in China.

Herein lies one of the biggest causes of confusion when it comes understanding the system. Journalists and commentators have wrongly conflated the proposed Social Credit System with the Sesame Credit pilot scheme. The private company pilot schemes for financial scoring have been

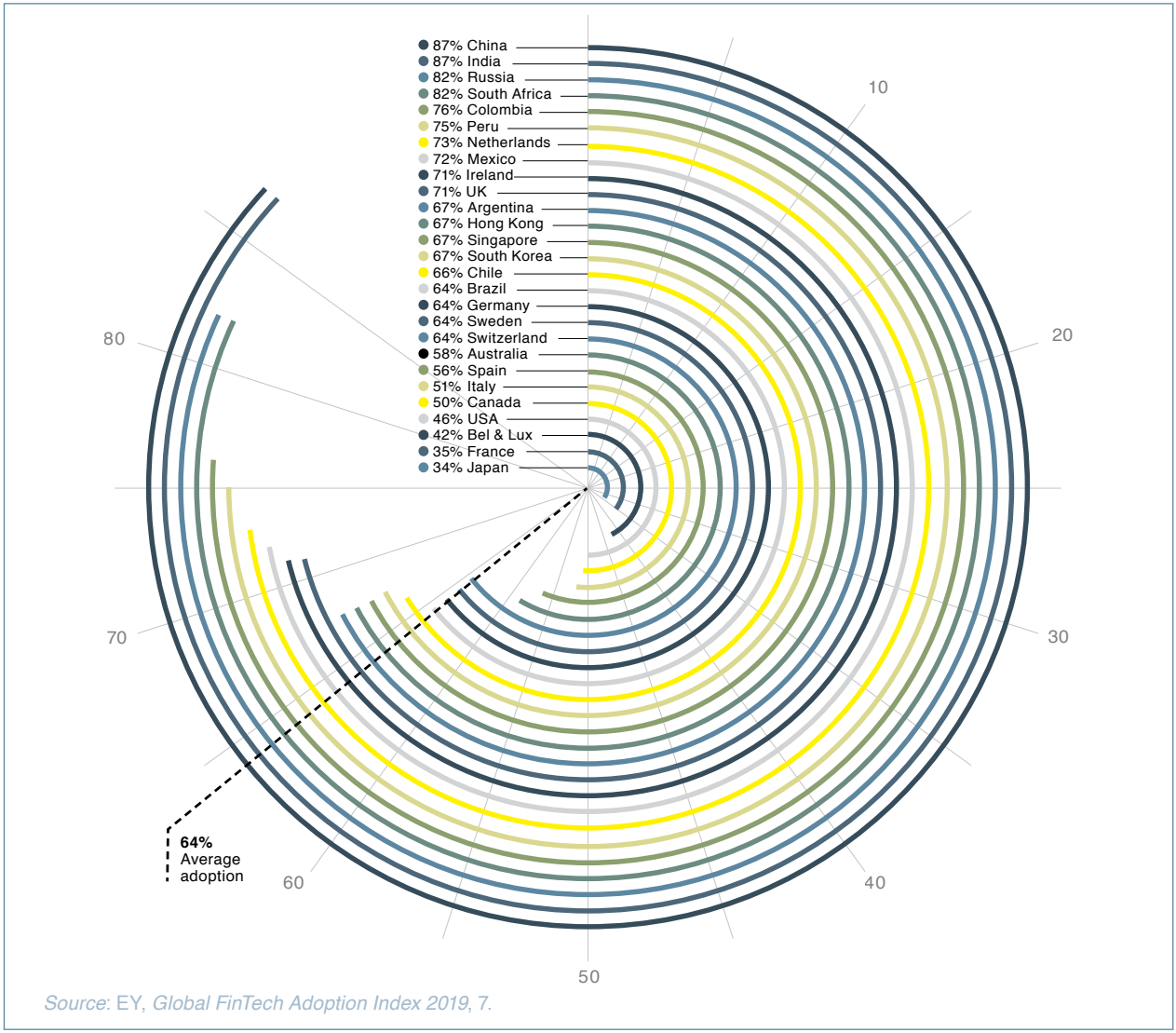
[59] L. Matsakis, 'How the West Got China's Social Credit System Wrong', *Wired*, 29 July 2019.
[60] N. McCarthy, '1.7 Billion Adults Worldwide Do Not Have Access to a Bank Account', *Forbes*, 8 June 2018.
[61] J. Daum, 'Social Credit Overview Podcast', China Law Translate, 31 October 2018.

depicted as one comprehensive system with dynamic scoring that monitors overall behaviour on the national level. As noted by one expert on Chinese social credit: 'What happened is some of the media took the private pilots, like Sesame Credit . . . and presented it as the social credit system'.[62] In 2018 the People's Bank of China decided not to renew the eight companies' licences to pilot these schemes and declined to proceed with any of them due to potential conflicts of interest. Sesame Credit and the other pilot schemes remain in operation as private services for their customers and can be viewed as loyalty programmes for their users, who can take advantage of potential perks or even boast about their high ratings on social media or dating websites. In late 2017 Hu Tao, the General Manager at Sesame Credit, wrote an open letter to reassure members of the public that the company's scoring product is an independent, third-party service which does not share user scores or data with the government, nor monitor personal behaviour.[63] The company firmly denies the assertion that its service is an extension of the government's Social Credit System.

This being said, it is an open question as to whether the government can tap into the personal data of the users of these credit reporting schemes should it wish to obtain individual information. As seen in the previous section of this paper, the line between private companies and the central government is blurred. Even though the private credit schemes claim to be independent and separate from the public Social Credit System, it remains to be seen in what direction these private initiatives will develop in the future. In recent years, China has been one of the top countries globally when it comes to the adoption of financial technology services—almost all digitally active users have used innovative products or services (Figure 3).[64] Two payment platforms, Alipay and We Chat Pay, account for 94% of the mobile payments market in the country.[65] Given the mass adoption of mobile financial services and growing individual reliance on mobile devices, the Chinese authorities will be more than interested in being able to tap into such data and to openly or covertly integrate private companies' information into the future design of the Social Credit System.

[62] Matsakis, 'How the West Got China's Social Credit System Wrong'.
[63] H. Tao, 'Zhima Credit Does Not Share User Scores or Data', *Financial Times*, 15 November 2017.
[64] EY, *Global FinTech Adoption Index 2019* (June 2019).
[65] Bank for International Settlements, *BigTech and the Changing Structure of Financial Intermediation*, BIS Working Papers no. 779 (April 2019), 6.

Figure 3 Consumer financial technology (FinTech) adoption across 27 countries



Source: EY, *Global FinTech Adoption Index 2019*, 7.

National implementation: the joint punishment system

The Chinese Social Credit System can be regarded as an attempt to incorporate administrative, technical and financial instruments into an integrated system for safeguarding individual and organisational compliance. The idea is for every citizen or organisation to have an expanding record of available data. Information collection, consolidation and aggregation are key here, rather than individual scoring.[66] Social Credit uses the national identity numbers of Chinese citizens and the identification codes of companies to keep synchronised records. The Social Credit Planning Outline envisages incentive and punishment mechanisms as the bedrock for ensuring lawful behaviour in a synchronised system that is run through the various administrative departments. If a person or organisational entity breaks laws or regulations, they risk being placed on integrated blacklists. These punishment provisions were in development even before Social Credit came about—in 2013 the Supreme People's Court issued a regulation to create a comprehensive blacklist system within the country.[67] An individual or organisation that has failed to implement a binding court or administrative decision can be put on a public blacklist for a specific period of time. Removal from the blacklist is only possible after an additional court decision.

These blacklists have become an integral part of the Social Credit System. In 2016 various party bodies, administrative departments and public institutions produced a memorandum of understanding which clarifies their respective roles in enforcing these blacklists in a scheme which is known as the Joint Punishment System.[68] The memorandum[69] lists potential punitive measures that can be taken against organisations or individuals and how the different administrations would synchronise their actions and cooperate to implement the punishments. For businesses and their legal representatives,

[66] J. Daum, 'China Through a Glass, Darkly', *China Law Translate*, 24 December 2017.
[67] R. Creemers, 'Some Regulations Concerning Publishing Name List Information of Persons Subject to Enforcement for Trust-Breaking', *China Copyright and Media*, 8 November 2016.
[68] Creemers, 'China's Social Credit System', 14.
[69] Ibid., 31.

the penalties include restricted access to government subsidies and loans; limited opportunities to establish companies, issue bonds or purchase property; and numerous other provisions. After breaking a court order, individuals can be barred from leaving the country, buying plane or high-speed rail tickets, making luxury purchases, or making other types of personal expenditures or economic investments. The Joint Punishment System is already showing its teeth. According to the annual report of the Chinese National Public Credit Information Centre, 17.5 million people had been restricted from buying plane tickets and a further 5.5 million had been denied high-speed rail tickets by the end of 2018.[70] The report further lists numerous instances of individuals being denied senior management positions within companies or being blocked from leaving the country because of unpaid taxes or related offences. The blacklist system synchronises information sharing between administrative bodies, judicial organs and market entities to ensure the ability to apply wide-ranging punitive measures which can impact various aspects of an individual's daily or professional life.

In essence, the blacklists establish a new type of government punishment that lies between the private sector and the state administration and involves a growing number of state departments and private companies.[71] The punitive measures also rely on an extra layer of reprimand—the blacklists are available online and are also disseminated through the mass media in China to ensure the public naming and shaming of offenders. It can be argued that the blacklist system is an extra-legal scheme as it imposes additional punishments and runs in parallel to the national justice system, with unclear sources of functioning appeal or redress. Human Rights Watch has previously reported the arbitrary inclusion of individuals on blacklists without prior notification, and their being forced to go through byzantine administrative procedures with uncertain outcomes.[72] The increasing integration of individual or company data, together with a potentially extra-legal mechanism for providing punishments across the board, opens the door for silencing dissidents and abusing human rights.

An important issue is also whether the completed system will fully apply to foreign nationals residing in China on a long-term basis. This might raise a number of questions for European citizens, who could find themselves embroiled in the complex web of the Chinese Social Credit System.

[70] L. Kuo, 'China Bans 23m From Buying Travel Tickets as Part of "Social Credit" System', *The Guardian*, 1 March 2019.
[71] M. von Blomberg, 'The Social Credit System and China's Rule of Law', *Mapping China Journal* 2 (2018), 89.
[72] M. Wang, 'China's Chilling "Social Credit" Blacklist', Human Rights Watch (12 December 2017).

Local Social Credit pilots and public opinion

Given the ambitiousness of the effort, the Chinese leadership has decided to let provincial administrations run their own social credit pilots, while at the same time working on the above-mentioned national system for implementing punishment. Currently there are over 40 pilot social credit experiments ongoing, which have been supplemented by provincial and municipal legislation.[73] The design and scope of these local pilots varies across the different provinces and all of them remain in development. An oft-cited example is the scheme in the city of Rongcheng, where people are assigned a grade from AAA to D that reflects their public misdeeds or exemplary behaviour.[74] If a person is caught jaywalking or littering, they can be sanctioned, which can lead to their grade falling, whereas communal engagement or volunteering for specific causes can increase their grade. The system can also be seen as a way to record violations of regulations and is fed with data from the local administration, social organisations and volunteers.[75] An additional example is the Honest Shanghai phone application, developed by the Shanghai Municipal Government. Citizens can input their government identification number and receive an assessment of their records based on government data—only small rewards are provided and use of the application is optional.[76] It is interesting to note that even though there is a technological component to these local examples, the majority of the data on record is collected manually—administrators fill in voluminous paper files or digital spreadsheets to update personal records. One of the government's aims is to digitise most of this information and improve coordination between state administrations for the optimal implementation of the system. As stated above, the ability to integrate private-sector applications or user data in the design will be crucial in the future.

[73] D. Síthigh and M. Siems, *The Chinese Social Credit System: A Model for Other Countries?*, European University Institute Working Papers, LAW 2019/01 (January 2019), 14.

[74] M. Ohlberg et al., *Central Planning, Local Experiments. The Complex Implementation of China's Social Credit System*, Mercator Institute for China Studies (12 December 2017), 12.

[75] For a more comprehensive explanation of the Rongcheng experiment, see J. Daum, 'Getting Rongcheng Right', *China Law Translate*, 29 March 2019.

[76] Ohlberg et al., *Central Planning, Local Experiments*, 12.

How are Chinese citizens responding to these systems? A 2018 public opinion study focused on citizen approval of the Social Credit System. One of the findings was that Chinese people are highly engaged with private credit scoring systems such as Sesame Credit (58%), but only 7% of citizens reported that they were part of a state-run local pilot for social credit.[77] This shows that the Chinese Social Credit System is still relatively unknown among the general population as it is still in development. An additional key insight from the study was that 80% of the respondents either strongly or somewhat strongly approved of the use of social credit systems.[78] Some might question the validity of the study, given that the respondents might have been discouraged from replying honestly out of fear of speaking out against governmental projects. The approval record might also stem from high levels of techno-optimism in Chinese society, which might see such systems as a positive technological advancement or an opportunity to benefit personally. The strong approval rating from different demographic and income groups implies that Chinese citizens are unlikely to oppose the future development of social credit applications. The lack of strong civil society organisations, independent privacy watchdogs or investigative media in China means that the general public will not be made aware of the potential risks of the system. Even though the aforementioned opinion poll cannot give us conclusive evidence about citizens' actual understanding of the issue, one might conclude that state media and governmental efforts have been successful in convincing many people of the need for and benefits of a social credit system.

Social Credit and businesses: implications for European companies

An important aspect of the Social Credit System is its consequences for private companies and its likely future impact on European businesses operating in mainland China. The potential relationship

[77] G. Kostka, *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval*, SSRN (23 July 2018), 11.
[78] Ibid., 11.

between the system and foreign companies is crucial as it may mean that the Social Credit System would not stop at the Chinese border but could influence the operations of international businesses.

The Social Credit System for Companies is based on the same premise as that for individuals—the massive collection and evaluation of data from different governmental bodies, leading to potential rewards or punishments for businesses. Relevant indicators include registered judicial complaints, respect for applicable regulations, tax obligations, corporate social responsibility, environmental standards and many others. Earlier studies of the corporate aspect of social credit have suggested that, if it is successful, the system has the potential to become 'the most globally sophisticated and fine-tuned model for big-data enabled market regulation'.[79] That said, it must be emphasised that the corporate system has also not been fully implemented in China and many of its components are still works in progress which will surely continue beyond 2020.

The corporate extension of the system has already started raising red flags and has caught the attention of the EU Chamber of Commerce in China, which has published an extensive report on its implementation and the potential far-reaching consequences for European companies.[80] The report notes that a Chinese consortium comprising, among others, Huawei, Alibaba, Tencent and a video surveillance provider is setting up a new meta-database for the fully integrated monitoring and reporting of company performance for all national and foreign companies in China.[81] The successful operation of the system might incentivise having a good company track record through rewards such as lower taxes or more favourable credit conditions, but it could also sanction businesses through higher taxes, targeted audits or additional inspections due to poor performance. Theoretically a wide-ranging monitoring system could provide a level playing field for companies and increase overall compliance with government regulations and safety standards. However, there are serious concerns that the system might discriminate against international companies and give unfair advantages to national firms which might benefit from direct support or information flows from government administrations.[82] Potential

[79] M. Meissner, *China's Social Credit System: A Big-Data Enabled Approach to Market Regulation With Broad Implications for Doing Business in China*, Mercator Institute for China Studies (24 May 2017), 11.

[80] European Union Chamber of Commerce in China and Sinolytics, *The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors* (August 2019).

[81] Ibid., 5.

[82] Ibid.

discrimination against foreign companies is just one side of the coin. An effective corporate social credit scheme might also try to push European and international businesses to comply with certain political or technical provisions which are prescribed directly by the CPC. The chief executive of the consulting firm which helped to draft the European Chamber's report has commented that corporate social credit 'is a very, very potent instrument for regulating, controlling and steering companies in a targeted way'.[83]

Nudging international companies to comply with the Chinese Politburo's dicta is definitely not just a theoretical possibility. In 2018 the Chinese Civil Aviation Administration accused international airlines of 'serious dishonesty' and the violation of Chinese laws due to their listings of Taiwan, Hong Kong and Macau as destinations on their websites.[84] According to China scholar Samantha Hoffman, the airlines were accused of violating specific measures which implemented two key policy guidelines of the Chinese Social Credit System.[85] This early precedent shows how social credit can be used as a direct threat to compel companies to toe the CPC line if they do not want to be sanctioned.

This is just a glimpse of the potential implications of a fully functioning corporate social credit system for foreign companies. Traditionally, EU businesses have had difficulty penetrating the Chinese market or have been compelled to operate through joint ventures. A fully integrated corporate social credit system might make the daily operations of European businesses even more difficult by requiring them to report vast amounts of company data, and could potentially discriminate against them due to political pressures. European businesses might be pushed not only to comply with existing legal obligations but also to follow the official party line and adhere fully to top-down political provisions. The president of the EU Chamber of Commerce in China succinctly concluded that this system could be the 'life and death of European companies'.[86] Most worryingly, it appears that the Chinese corporate system could transcend national borders and aim to influence global discourse by applying pressure on international businesses and even foreign governments.

---

[83] M. Martina, 'Business Group Issues Wake-up Call on China's Corporate "Social Credit" Plan', *Reuters*, 28 August 2019.
[84] J. Rogin, 'White House Calls China's Threats to Airlines "Orwellian Nonsense"', *Washington Post*, 5 May 2018.
[85] S. Hoffman, *Social Credit Technology—Enhanced Authoritarian Control With Global Consequences*, Australian Strategic Policy Institute, Report no. 06/2018 (June 2018), 3.
[86] European Union Chamber of Commerce in China and Sinolytics, *The Digital Hand*, 1.

The Chinese Social Credit System: a recap

It is easy to get lost in the design and rationale of the Chinese Social Credit System. The numerous local administrative pilots in the Chinese provinces and the implications for individuals, businesses and national administrations make it arcane and extremely complex. For the time being, social credit should not be seen as an omnipresent highly technological system that generates a dynamic score based on intricate algorithms. Rather, it is an administrative push to ensure regulatory enforcement through improved synchronisation between different levels of bureaucracy. This system can impose sanctions on individuals or organisations in cooperation with the whole administrative apparatus and even private companies, which play a role in the implementation of penalties (e.g. where individuals are denied the right to purchase plane or train tickets). Some scholars have described the system as the digital revival of the Maoist *dang'an* (record) system—this was a paper file held by the government that included school reports, employment records, photos and personal information which was used to monitor and profile individuals.

Social credit is no blunt administrative tool. Even though it is neither completely operational nor fully optimised technologically, its importance should not be underestimated. Increased government scrutiny, public shaming and blacklists with severe penalties—all are signs that the system is growing and certainly has teeth. One has to seriously consider the main goal of the system, that is, to restore 'trust' within a 'harmonious' socialist society. Ultimately, it is the CPC and its subordinates that define 'trustworthiness' or acceptable conduct within society. All the local pilots and increased efforts to share information have the goal of nudging individual or company behaviour in the right direction and keeping it in line with the Communist establishment.

There are clear indications that the design and implementation of the Social Credit System in China will continue beyond 2020 and extend deep into the decade. In the coming years big data, cloud technologies and automated systems would be able to expand this framework into many domains of

everyday life, tie social credit to China's surveillance apparatus and even obligatorily incorporate it into the technological products of private companies. The Social Credit System could eventually be extended beyond Chinese borders by coercing foreign businesses to comply and by effectively shaping the global discourse on China. Even though it is still in development, the Chinese Social Credit System is one of the likely future hubs of Beijing's digital authoritarianism.

In closing, an important note is in order. Many media reports and pundits have described the planned Social Credit System as the ultimate dystopian tool which imposes algorithmic governance on Chinese society. In a way such a concept may correspond with our own nightmarish visions of an all-seeing panopticon and personal fears about the exploitation of advanced AI. However, for the time being this system remains far from being such an optimised mechanism. Social Credit System or otherwise, the government already has the necessary tools to monitor individuals, study their behaviour and gain direct access to private communications. Digital authoritarianism is already present in China and even if the Social Credit System fails to be implemented fully, this will not be the end of censorship, surveillance and oppression. This is a valuable reminder for European citizens as well—you do not need to wait for such a system to become fully operational in another country in order to be concerned about the management of personal data or unlawful surveillance.

Exporting oppression: the global spread of digital authoritarianism

In the last decade China's digital authoritarianism practices have been widely documented and criticised by human rights organisations, international media and national governments. The usual response from Chinese authorities to such rebukes is either silence or a complete disregard of these concerns, given that the sovereign state of China is free to determine its own policies. However, Chinese digital authoritarianism is no longer solely a domestic issue. Through its digital champions, through its trade and development policies, and even through its international 'sharp' power,[87] China has started to export its digital authoritarianism model globally. These efforts are mostly aimed at Asian states or developing countries in Africa and Latin America. Many of these states have lower institutional resilience to external influences, or are extremely optimistic about economic deals with China that promise connectivity infrastructure, technological partnerships, or large-scale development projects that guarantee financial and employment opportunities. Such projects are accomplished primarily through Beijing's flagship 'Belt and Road' initiative for large-scale projects with numerous stakeholders or through bilateral partnerships with various countries. Europe has not remained unscathed when it comes to these efforts. The Chinese '17+1' platform engages with Balkan, Central and Eastern European countries with the promise of infrastructure investment and technological advancement, but comes at the expense of European unity, as well as increased dependence on Chinese hardware and software. Additionally, Chinese tech and telecoms companies are expanding their global reach when it comes to the fifth-generation (5G) mobile network roll-out and the export of AI and facial-recognition software, as well as surveillance technologies, all of which raise grave cybersecurity concerns and additional fears about the institutionalisation of human rights violations across the globe.

The Belt and Road Initiative and its digital grip

The Belt and Road Initiative (BRI) was announced by Xi Jinping in 2013 as a flagship Chinese project for reviving ancient trade routes globally by improving the economic and infrastructure development of

[87] 'Sharp' power can be understood as a complex diplomatic, media and cultural strategy which engages in distraction and manipulation in order to shape public opinion internationally.

partnering nations. Through parallel projects in different economic corridors, China aims to bridge the huge infrastructure investment gap in partnering countries and, ultimately, boost its own economic and diplomatic interests. The expanding Chinese agenda can also be seen as an attempt to revamp the rules of the international economy by reordering global value chains.[88]

As of late 2019, more than 100 countries had expressed interest in or signed BRI partnerships—the reach of the initiative touches two-thirds of the world's population.[89] China has pledged to continue the BRI as an umbrella initiative throughout the 2020s and has committed at least $1 trillion in funding. This ambitious platform is largely funded by the China Development Bank and the Export–Import Bank of China, both of which provide attractive loan options. Without a doubt, the BRI is a boon for developing countries that are suffering from poor energy, telecoms and road infrastructure, as well as low GDP per capita. However, there is growing criticism that the platform lacks transparency and that its specific parameters for concluding partnerships, allocating loans and choosing contractors are unclear.[90] The biggest problem is the rise of 'hidden debts' as many of the financial flows related to the project are not reported to the IMF or the World Bank.[91] There is notable concern that China is indebting dozens of countries which are unable to repay their loans and could be placed under pressure to provide political favours to Beijing in the long run. EU member states have criticised the project as it runs against liberalised global trade and solely promotes the interests of heavily subsidised Chinese companies.[92]

One of the main pillars of the BRI is the 'Digital Silk Road'—the digital division of the initiative—which focuses on investment in broadband networks, data centres, long-distance fibre-optic cables and related digital infrastructure. Estimates suggest that under this heading China has invested $79 billion[93] in projects around the globe, primarily in Southeast Asia and Africa. In effect, China is heavily involved in building the digital backbone of many developing countries, which are expressing a growing interest in cheap and functional technological advancement. Relevant examples of these projects include

[88] B. Mações, *China's Belt and Road: Destination Europe*, Carnegie Europe (9 November 2016).
[89] China Power, *How Will the Belt and Road Initiative Advance China's Interests?*, Center for Strategic and International Studies (8 May 2017).
[90] C. Campbell, 'China Says It's Building the New Silk Road. Here Are Five Things to Know Ahead of a Key Summit', *Time*, 12 May 2017.
[91] S. Horn et al., *China's Overseas Lending*, The National Bureau of Economic Research, Working Paper 26050 (July 2019).
[92] D. Haide et al., 'EU Ambassadors Band Together Against Silk Road', *Handelsblatt Today*, 17 April 2018.
[93] S. Prasso, 'China's Digital Silk Road is Looking More Like an Iron Curtain', *Bloomberg*, 10 January 2019.

data centres in North Africa[94] and underground/underwater fibre-optic cables in Pakistan, Vietnam, Indonesia and the Philippines, to name just a few.[95] This approach is extremely prescient as it further reinforces Beijing's strategy of tech dominance. Chinese companies are set to dominate these countries' information and communications technology infrastructures, limiting the ability of local or Western companies to compete in the long run. What is more, China is making these countries path dependant on future hardware or software support provided by Chinese firms. China will also be tempted to tap into the valuable troves of data created and open new avenues of covert intelligence collection. Beijing has a proven track record in such notorious practices. An investigation[96] by French daily newspaper *Le Monde* proved that China siphoned off confidential data from the Chinese-built IT network set up in the African Union's headquarters between 2012 and 2017.

Cybersecurity and the interception of data are only part of the concern. These countries receive more than loans and technological equipment—they are heavily influenced by China on how best to utilise them and what regulatory policies to develop in parallel. In 2018 China hosted sessions on its 'best practices' in censorship and surveillance for representatives from Morocco, Egypt and Libya.[97] Similar country-specific trainings were organised in Saudi Arabia, the United Arab Emirates, the Philippines, Thailand and Vietnam in 2017-18. Beijing is cultivating media elites to create a favourable group of countries which might follow its Internet policy.[98] Vietnam's ensuing adoption of a cybersecurity law which closely mimics China's legal framework is a telling example of Beijing's influence on national legislation. Indeed, it seems as if the 'Digital Silk Road' provides the full package for China's partner countries—not only the infrastructure and hardware, but also the digital authoritarianism playbook from which others can copy.

[94] T. H. El Kadi, 'The Promise and Peril of the Digital Silk Road', Chatham House, The Royal Institute of International Affairs (6 June 2019).
[95] B. Harding, 'China's Digital Silk Road and Southeast Asia', Center for Strategic and International Studies (15 February 2019).
[96] J. Tilouine and G. Kadiri, 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin', *Le Monde*, 26 January 2018.
[97] El Kadi, 'The Promise and Peril of the Digital Silk Road'.
[98] A. Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (October 2018), 8.

Safe cities and surveillance technology

In the last several years China has actively promoted business partnerships with many countries globally, either through current BRI projects or as separate bilateral deals, for the export of cutting-edge surveillance technology and related software. Under the label of 'Safe Cities' or 'Smart Cities', the Chinese company Huawei has been selling a wide array of products globally: smart surveillance cameras, facial- and licence-plate-recognition software, crowd monitoring, cloud-based video surveillance and even command centres for cross-agency collaboration.[99] The dissemination of Huawei's products has been considerable—the company has stated that it introduced such smart city technologies to 40 countries in 2017[100] and that by 2019 the number of partnering countries had at least doubled.[101] This equipment is either directly bought or provided on loan from China with the aim of increasing public safety and reducing crime. While this technology has the potential to increase public safety, recent research shows that the benefits of Huawei's technology are difficult to verify and even appear exaggerated in some cases.[102]

It should be emphasised that China is rolling out these products in countries not only with less-developed technological infrastructures but which also have poor human rights track records and illiberal regimes of governance. More than half of these partnerships are with African or Asian countries and the majority are with countries which have been listed as 'partly free' or 'not free' by Freedom House in the last decade. The *Freedom on the Net 2018* repor notes that China has supplied all of these technologies 'to a variety of governments with poor human rights records, which could benefit Chinese intelligence services as well as repressive local authorities'.[103] It must be added that smart cities partnerships or Chinese projects for the city-wide management of interconnected

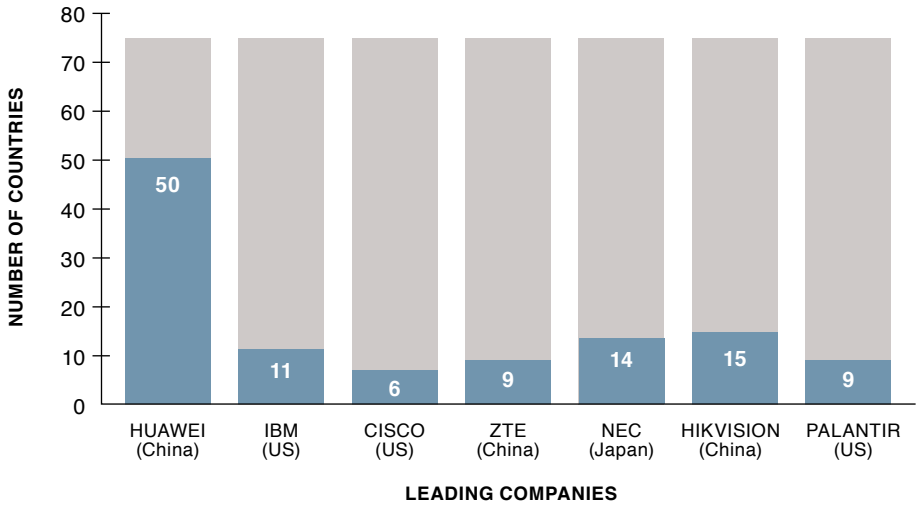
[99] Many of these products are listed on Huawei's dedicated webpage: https://e.huawei.com/us/solutions/industries/public-safety.
[100] Huawei, 'Huawei Creates a Smart City Nervous System for More Than 100 Cities with Leading New ICT', Press release (14 November 2017).
[101] D. Cave et al., *Mapping China's Tech Giants*, Australian Strategic Policy Institute (18 April 2019), 10.
[102] J. E. Hillman and M. McCalpin, 'Watching Huawei's "Safe Cities"', Center for Strategic and International Studies, CSIS Briefs (4 November 2019).
[103] Shahbaz, *Freedom on the Net 2018*, 2.

devices are present in European member states as well. Huawei has developed smart city projects with local administrations in Germany, Italy and Malta, with these European governments asking very few questions about the associated potential risks of such partnerships.[104]

As of late 2019 China is the global leader in AI surveillance technology exports. The AI Global Surveillance Index recently closely examined the worldwide spread of AI surveillance tools such as 'safe cities', facial-recognition systems and smart policing.[105] Findings show that at least 75 out of 176 countries globally are actively using AI technology for surveillance purposes and this spread is evident in a variety of countries with different levels of development and political systems.[106] A mix of Chinese companies is supplying surveillance technology in 63 countries, with Huawei alone supplying at least 50 of them (Figure 4).[107] Of course, the presence of such technologies in these countries does not necessarily directly imply that they are being used for unlawful surveillance or espionage. However, independent investigations give enough grounds to raise concerns about the utilisation of Chinese surveillance tech in some of these states.[108] The autocratic governance in many of these countries or their poor human rights records implies that much of this technology can be abused. Similar caution has to be applied to the Chinese firms providing these exports. In this case we are not discussing the large-scale market penetration of classic private companies which seek purely economic profit. As seen in the first section of this paper, there is a series of questions about Chinese tech companies' relationship with the state, as well as their ownership structures, which calls into serious doubt their status as fully independent private entities.

[104] Shi-Kupfer and Ohlberg, *China's Digital Rise*, 38.
[105] S. Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace (September 2019).
[106] Ibid., 7.
[107] Ibid., 1.
[108] J. Parkinson et al., 'Huawei Technicians Helped African Governments Spy on Political Opponents', *The Wall Street Journal*, 15 August 2019.

Figure 4 Leading companies contributing to AI surveillance



Source: S. Feldstein, *The Global Expansion of AI Surveillance,* Carnegie Endowment for International Peace (September 2019).

The direct spillover of both the Digital Silk Road and the commercial sale of surveillance technology is the global spread of digital authoritarianism. It does not matter whether this spillover is intentional or unintentional. It opens the door for the institutionalisation of unlawful surveillance, the suppression of universal human rights and the downfall of democratic values. It may also perpetuate the rule of authoritarian regimes in other countries and become a tool of oppression for use against minorities or political opposition. This strategy is a direct challenge to the national security of sovereign nations and could lead to cybersecurity breaches, increased cyber-attacks and widespread espionage. The international community, and especially the transatlantic alliance, must urgently recognise these threats and develop a comprehensive approach to the deterrence of digital authoritarianism.

Box 2 A glimpse of Chinese digital authoritarianism abroad

Venezuela

A 2018 Reuters investigation showed the central involvement of a Chinese company in developing and implementing the Fatherland Card (Carnet de la Patria), which is a digital record of personal data, property ownership, employment and even political affiliation.[109] The Chinese telecoms company ZTE was instrumental in the implementation of what is essentially a tracking programme for political and economic behaviour. Even though use of the card is voluntary, a large chunk of the population has been encouraged to get one through the application of economic incentives and government subsidies. Most strikingly, the card was used during the 2018 elections when voters were asked to register their card before voting, which led to the widespread rumour that the government was tracking whether people had voted for Maduro. The same company is additionally providing technical and training support to Venezuela's government-run telecoms company Cantv.[110]

Zimbabwe

As part of the BRI, China and Zimbabwe signed a cooperation agreement in 2018 for the provision of a widespread facial-recognition programme in the African country including closed-circuit television cameras, smart financial systems and a national facial database.[111] China has a history of supporting Zimbabwe's authoritarian regime but this deal comes with a twist. The African state is expected to share the biometric data of millions of its citizens with China so that Chinese companies can improve their algorithms' recognition and classification of people with black skin. Studies show that AI facial-recognition software registers the lowest error rates when attempting to identify lighter-skinned individuals compared to attempts to

[109] A. Berwick, 'How ZTE Helps Venezuela Create China-Style Social Control', Reuters Special Report (14 November 2018).
[110] A. Berwick, 'Service? Don't Rely on Venezuela's State Telecoms Firm Cantv', *Reuters*, 23 November 2018.
[111] A. Hawkins, 'Beijing's Big Brother Tech Needs African Faces', *Foreign Policy*, 24 July 2018.

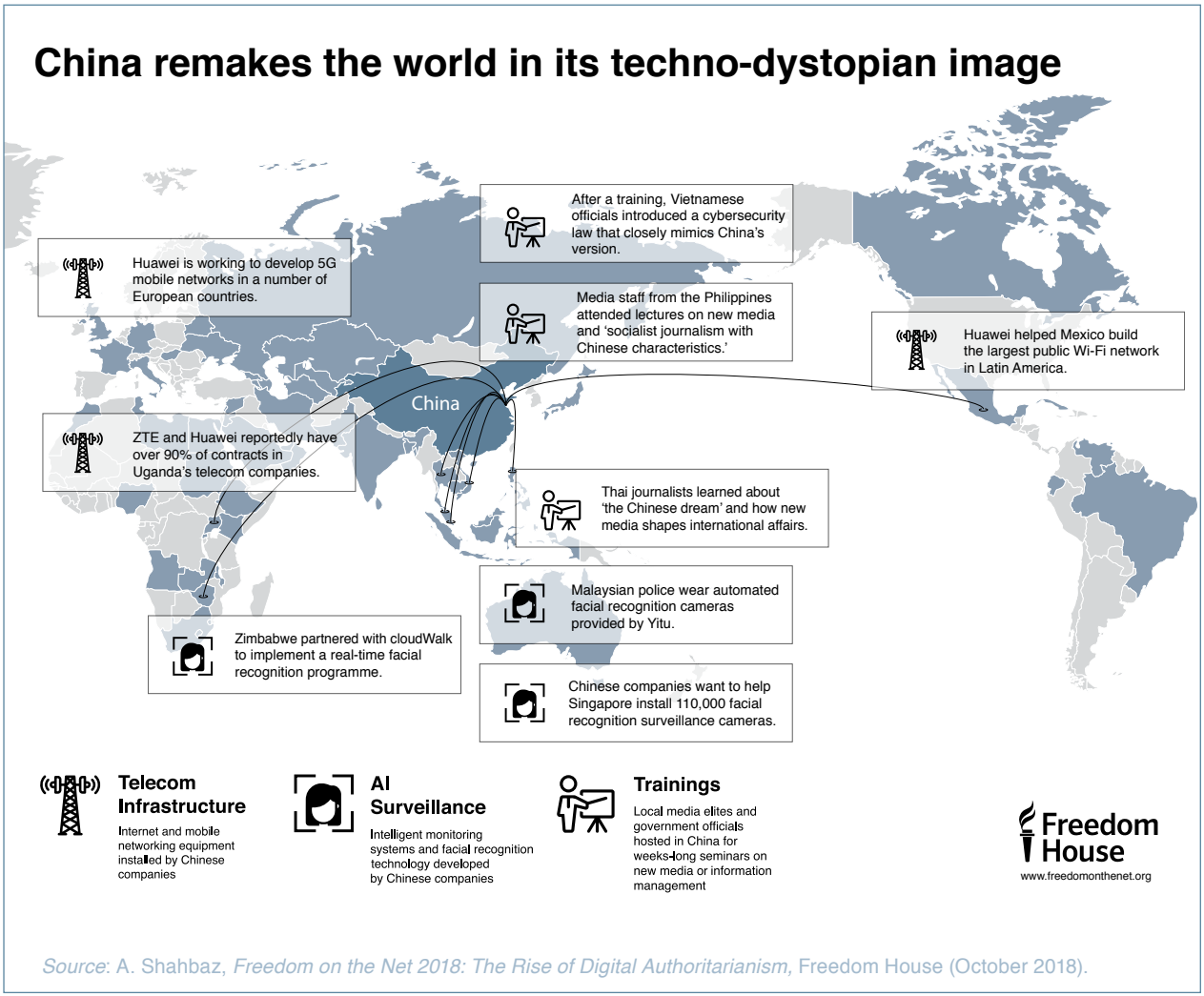
identify darker-skinned people.[112] Experts have suggested that this partnership will not only expand authoritarian practices in Zimbabwe but also help China accumulate raw biometric data for its own gain—a new form of 'data colonialism'.[113]

Ecuador

China has assisted Ecuador with building its ECU-911 system to help local law enforcement fight crime. The system involves elaborate video-surveillance equipment which monitors various parts of the city. A report by *The New York Times* shows how Ecuador's intelligence agency has direct access to the system and is potentially exploiting it to monitor its citizens.[114]

[112] J. Buolamwini and T. Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research* 81 (2018).
[113] F. Ryan et al., 'Mapping More of China's Technology Giants', Australian Strategic Policy Institute (November 2019), 13.
[114] P. Mozuer et al., 'Made in China, Exported to the World: The Surveillance State', *The New York Times*, 24 April 2019.

Figure 5 Tactics employed by China in the spread of digital authoritarianism



Source: A. Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism,* Freedom House (October 2018).

Implications for the EU

What are the most important repercussions for European member states? First of all, cyber independence and the overall Chinese model described in this paper have started to directly compete with Europe's attempt to pioneer a landmark framework for data protection and the safeguarding of individual rights online. The EU is trying to strengthen online privacy through the design, confidentiality and security of electronic communication and even to pre-empt the potential harm of the unregulated application of advanced AI capabilities. Partial criticism of some aspects of Europe's approach aside, it must be noted that the EU is attempting to find a balanced and human-centric solution to one of the most pressing challenges of this century. It appears that the People's Republic of China is going in precisely the opposite direction.

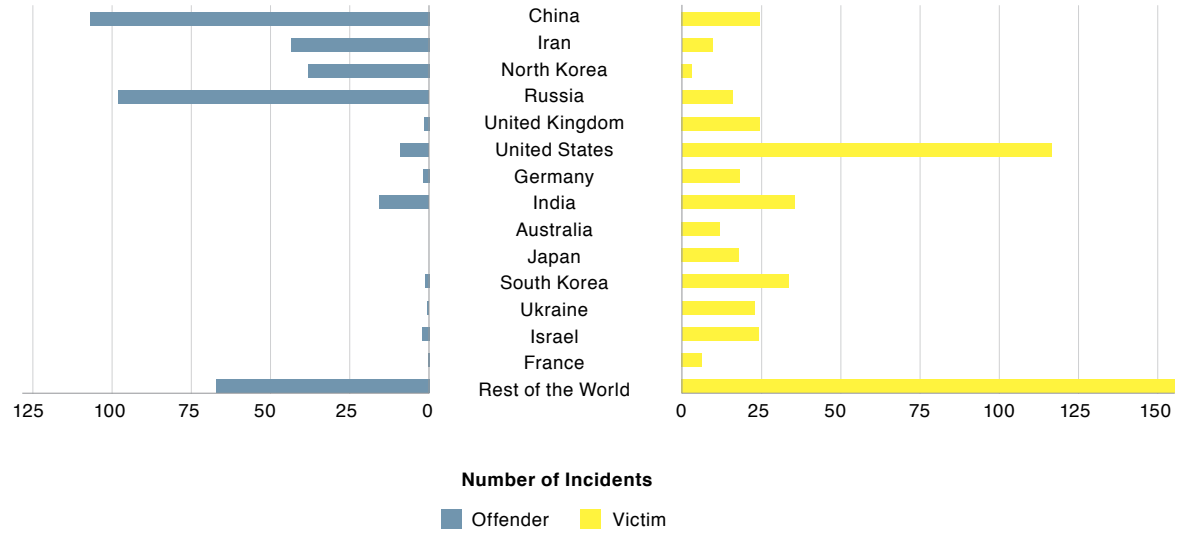
Through political clout or economic influence, Beijing is recruiting numerous other international actors to subscribe to its model and support China's behaviour in international fora or multilateral institutions such as the UN. A case in point is the backlash against the UN Human Rights Council letter signed by 22 states condemning the aforementioned Chinese oppression in Xinjiang. In response, Saudi Arabia, Russia and 35 other states produced a joint statement praising China's human rights efforts.[115] This is just one example among many. As stated before, many countries and their citizens might benefit from China's involvement in infrastructure and connectivity projects under the BRI. However, this cannot come at the price of intentional secrecy, unsustainable debts and political coercion. Additionally, the 'Digital Silk Road' and parallel Chinese foreign policy objectives can only be met with European condemnation as they are effectively weaponising the Internet, institutionalising online censorship and surveillance, and luring many other states to follow suit in opposition to Western liberal democracies.

Second, digital authoritarianism and its spillovers are a potential threat to European citizens in their everyday lives. There is a creep of corrupt Chinese technological and software products in the EU which poses a huge risk to sensitive personal data and overall European cybersecurity. On the

[115] M. Nichols, 'Saudi Arabia Defends Letter Backing China's Xinjiang Policy', *Reuters*, 19 July 2019.

face of it, this is nothing new. Expert research using publicly available information about the most significant cyber incidents (cyber-espionage and warfare) since 2006 shows that China tops the list with more than a hundred known offences (Figure 6). But this time it might get personal. Chinese border guards were recently exposed as having secretly installed surveillance applications on the personal phones of international tourists. This software can extract personal correspondence, images and device information.[116]

Figure 6 Significant cyber-attack and cyber-espionage incidents since 2006



Source: Centre for Strategic and International Studies, 'Significant Cyber Incidents' (2019).

[116] H. Osborne and S. Cutler, 'Chinese Border Guards Put Secret Surveillance App on Tourists' Phones', *The Guardian*, 2 July 2019.

Additionally, cheap Chinese Internet of Things (IoT) devices are quickly expanding their share in European markets where standards for these devices are still wobbly. The IoT sector is showing great economic potential, with billions of interconnected devices being purchased annually; however, the underlying security risks are also growing. Designated attacks on IoT devices have mushroomed in 2019, with 30% of the analysed attacks originating from China.[117] Earlier reports focusing on 2016 and 2017 show that the majority of the IoT attacks came from China then, as well.[118] Given the certain growth of Chinese IoT devices in the future, the IoT vulnerability situation is likely to deteriorate unless European policymakers intervene more effectively to set standards and ensure thorough safety checks.

On a different front, China has been under an additional spotlight due to security concerns related to Huawei's potential involvement in the roll-out of next generation 5G telecommunications technology in Europe. The US, Australia and New Zealand have all blocked the use of Huawei equipment for 5G purposes, citing security concerns. Throughout 2019 the EU was under substantial pressure to make a joint decision on the future involvement of the Chinese company in building 5G networks. European intelligence agencies have warned of the potential long-term risks stemming from a Chinese company building such crucial infrastructure and potentially manipulating or transferring valuable data at its government's request.

Lastly, Chinese tech giants are becoming a growing challenge to European businesses. Europe and its citizens would actually benefit from a healthy economic relationship with China. However, such a situation does not exist because of the constant mammoth subsidies provided by the Chinese government and the continuous protectionist measures that shield Chinese tech companies. Competition rules, the protection of intellectual property, security risks and data-related issues will continue to be thorny issues. Tensions may be further exacerbated, leading to Europe needing to make a series of difficult decisions. The growing influence of China and its companies in areas such as telecommunication networks, data centres, big data, quantum technologies and AI might be a heavy blow to European companies, which will likely cede ground to China as it conquers markets globally.

[117] S. Williams, 'Attacks on IoT Devices Booming, Research Finds', *SecurityBrief*, 24 October 2019.
[118] S. Boddy and J. Shattuck, *Threat Analysis Report: The Hunt for IOT – The Growth and Evolution of Thingbots Ensure Chaos*, F5 Labs (March 2018), 5.

Discussion and key takeaways

Digital authoritarianism in China is no future prospect. It is already here. Under Xi Jinping's rule the country has strengthened its grip on Internet freedoms and has made online monitoring and surveillance endemic. Through administrative reorganisation and updates to the relevant legislation, the People's Republic of China has **institutionalised draconian measures** for citizen surveillance and pervasive censorship, as well as gaining almost full control of online political discourse. Most worryingly, private tech companies have also been successfully woven into this complex web by reporting sensitive personal or behavioural data to the authorities on demand. The mass adoption of messaging, entertainment and financial digital applications by many Chinese citizens gives the authorities a formidable tool for individual monitoring and potential persecution. Large-scale **video-surveillance and facial-recognition** capabilities ensure that citizens are kept in check even if they are away from a digital device. And these systems need not be perfect or fully omnipresent in order to produce results. Most Chinese citizens presume that they can be monitored or reported on at any given time. This is the precise aim of the ruling CPC—ensuring constant self-censorship, crushing dissent in its infancy and guaranteeing the inevitability of the political system in the minds of its citizens.

The Chinese Social Credit System is an intricate extension of this tactic. It must be emphasised that its multiple pilot schemes, incomplete final design and opaque long-term goals leave much uncertainty. However, there is enough evidence to remain alert. A coordinated administrative system which feeds on data from different governmental sources and has the ability to sanction and publicly shame individuals would be a powerful tool in the hands of the Chinese Politburo. The new decade could bring further advancement of this system through the enhanced technological integration of data. An upgraded national social credit platform could make personal evaluations and punishments even more pervasive under the veneer of restoring 'trust' in society. Such a system could additionally encourage individuals to model their behaviour along the lines and conduct prescribed by the CPC.

As Chinese society moves to a growing dependency on mobile devices for online payments and financial transactions, government authorities can further exploit their skewed relationship with national tech companies and integrate such financial technology services into the future design of the Social Credit System. Big data and technological innovation can also be utilised to monitor businesses and increase behavioural nudging in the private domain. There is a substantial threat that a **corporate social credit system** might discriminate against European businesses or force them to comply with

even more stringent regimes for information and data sharing. Indeed, credit scoring, reputational ratings and loyalty programmes are known and have been developed in many democracies globally. However, the ambitions and complexity of a corporate social credit system might compel businesses and legal representatives not only to comply with existing regulations but also to follow the political imperatives of the CPC. The August 2019 report by the EU Chamber of Commerce in China raises worthy concerns about the risks for European businesses operating in mainland China and needs to be taken into consideration by European policymakers. Even though not fully synchronised, the national Social Credit System is still an extension of Beijing's practice of digital authoritarianism and might even become one of its central hubs in the future.

It is crucial to note that Beijing's efforts are influencing actors beyond its borders. This paper firmly acknowledges that **China is exporting its home-grown framework for digital authoritarianism globally**. This is a direct threat to the long-term interests of the EU and its international allies. Beijing is pursuing an active international endeavour to establish its cyber sovereignty doctrine as a clear alternative to the current open framework for Internet governance. It wants to see Internet restrictions, online censorship and limited digital privacy as the norm rather than the exception worldwide. This is an alluring prospect for authoritarian regimes and there is a growing body of evidence which demonstrates that other countries are copying directly from China's playbook. A notable concern in this regard is the **Russian Federation**. Moscow has already pursued its own brand of cyber independence and authoritarian online practices—Vladimir Putin's push for Russia to have its own 'independent' Internet has been widely reported. The Russian toolkit comprises blocking virtual private network servers, online censorship of civil society groups and illegal government surveillance through digital devices. Even though the country's progress remains a long way behind China's hi-tech systems for mass surveillance, Moscow could become a prominent ally in Chinese efforts to reshape the global online space. Given Putin's and Xi's positive personal relationship and the expanding bilateral ties in strategic sectors such as trade, energy and the military, a Sino-Russian cyber-independence alliance is all too likely to grow stronger in the future and become a model of influence for many other countries.

A new narrative for Internet governance is not the only thing being exported by China. The Chinese '**Digital Silk Road**', part of the flagship BRI, provides attractive loans and industrial support for the roll-out of essential digital infrastructure in dozens of developing countries in Asia, Africa and Latin

America. This ensures Beijing's entrenched position as a long-term supplier of communications technology and services in these countries. The former Asian empire can also abuse the skewed lender–creditor relationship by extracting political gains in exchange for its financial and technical generosity. In addition, Chinese companies are supplying cutting-edge AI surveillance technology and facial-recognition software to a growing number of developing countries, many of which have formed partnerships under the BRI. Intentionally or not, China is weaponising political regimes with repressive tools for surveillance and the suppression of political dissent. Democratic decay has already been recognised in a number of democracies globally, with political illiberalism mushrooming in parallel with the number of distinctly authoritarian systems. We are, indeed, a long way away from the coveted 'end of history'. These trends are a strategic threat to the EU and the North Atlantic alliance.

Such a statement merits a proper evaluation of the **overall direction of Chinese foreign policy** and its global engagement. The sections above detail the growing ambitions of China to (a) proactively shape global policy in strategic sectors, (b) claim manufacturing leadership by 2030, (c) become a powerhouse for AI and innovation, (d) revamp global trade and supply chains through the BRI, and (e) lay the digital backbone and information and communications technology systems for dozens of countries across several continents. We can see that Beijing has long since departed from Deng Xiaoping's famous '24-character strategy' of biding time and maintaining a low profile when it comes to Chinese foreign policy. For decades the Asian country has chosen to remain below the radar as much as possible and to focus on its internal matters and long list of domestic problems. Under Xi Jinping, however, the country is proactively seeking to rethink power relationships and become even more assertive on the global stage. Its stellar economic growth and booming internal market contribute to its growing political stature and regional hegemony. China's booming economy has contributed almost one-third of global growth in the last decade. Moreover, recent findings show that there has been an unprecedented expansion of the global middle class, with Asia accounting for a large chunk of the achieved increase[119] and China leading the continent's effort. This is also echoed in the newly found country narrative of 'the Chinese dream'—Xi's call to the nation for the optimism and dedication to achieve personal prosperity and homeland glory. All of these trends are also reflected in Chinese public opinion, as the vast majority of citizens approve of the direction in which the nation is headed and remain optimistic about the country's future.

[119] H. Kharas, *The Unprecedented Expansion of the Global Middle Class: An Update*, Brookings Institution (February 2017).

That being said, **one must remain sensibly critical of trending narratives about inevitable Chinese dominance** in economic, technological and global affairs. Recently, there has been much media hype and pundit overestimation of Chinese capabilities. China continues to be troubled by some of the problems facing a still-developing nation—the lack of basic infrastructure, food supplies and access to clean water remain a challenge for parts of the population. The country is plagued by widespread corruption, administrative inadequacies and the burdensome centralisation of power. China is far from technological independence and still relies on external supplies and existing value chains. The recent Sino-US trade spat and the American economic sanctions imposed on China's tech sector show that Beijing can still be exposed to crippling economic pain. Neither 'Made in China 2025' nor aspirations for world leadership in AI and breakthrough innovation are guaranteed to succeed. Such ambitious endeavours could fail like the many other government efforts in the past which relied extensively on centralised planning and heavy government involvement. Chinese demography is also a key variable in this complex equation. The country is expected to be hit by a severe demographic crisis in the late 2020s and throughout the 2030s as a result of its one-child policy. This will have negative implications for its labour force and economic competitiveness in the future. A more pessimistic scenario for China in the coming years involves a combination of stagnating economic growth, a freeze in income levels and an expanding demographic crisis. Interestingly, one might also deduce that such a grim possibility might actually push Chinese policymakers to increase their efforts to upgrade national industry and establish technological leadership, as these could serve as formidable advantages in tomorrow's world.

All of these developments **should raise numerous red flags for the EU and its member states**. Chinese digital authoritarianism is a direct challenge to European citizens and basic European values. It must be emphasised that China's new guise and changing international conduct may impinge on vital European interests and damage the Union's global standing. Some of Beijing's initiatives undermine EU member-state unity and weaken the EU's capability to respond collectively. Cheap IoT devices, 5G networks and even mobile applications from China continue to pose cybersecurity risks. If China does indeed manage to develop superiority in AI technology, quantum computing and advanced cyber capabilities, it would gain first-mover advantage in one of the most crucial areas for global influence. Not surprisingly, the 2018 French strategy for AI gloomily warns of the possibility of the EU becoming a digital colony of third-country tech giants. The EU needs to strengthen its own internal market and accelerate its catch-up in digital innovation and breakthrough technologies. If it does not take these steps, Europe risks becoming entrenched in a weaker position vis-à-vis China in the long-run.

It should be noted that all of these concerns should serve as a **reminder for EU member states and their global allies** to examine their own involvement in the potential proliferation of surveillance technology. The above-mentioned AI Global Surveillance Index reports that a considerable number of liberal democracies also use AI surveillance systems internally. Countries such as the US, France, Germany, Japan and Israel also supply surveillance equipment to third countries. Even though China remains the leader in the export of such equipment, other suppliers of this type of technology should not be excluded from scrutiny. Liberal democracies must make sure that they provide the necessary regulatory toolkit to address the mass market penetration of breakthrough technologies and to provide the essential safeguards for ensuring transparency, accountability and protecting fundamental human rights. Lastly, Europe needs to finally address the challenge from **third-country digital companies** (many of which American) and the exploitation of personal data, as well as the related risks of behavioural profiling and citizen surveillance. European consumers themselves have to consider the risks they are willing to take in exchange for digital convenience and personalised online entertainment in their daily lives.

As a new decade begins, the EU must make sure that its citizens have the necessary institutional and legal protection from abuses of modern technology such as facial-recognition software and the advanced application of AI. Neither ethical principles nor self-regulation by industry could successfully overcome such serious challenges. The EU must remain a global influence when it comes to ensuring a coherent regulatory approach to technology and stand ready to oppose the spread of digital authoritarianism.

Policy recommendations

This research paper can put forward a number of key recommendations for European policymakers. The EU must firmly acknowledge the threats stemming from the Chinese model of digital authoritarianism and ensure that the Union develops the necessary resilience and a long-term deterrence strategy.

1. The EU must increase international pressure on China for its inhuman treatment of Uighur Muslims and other minorities in the Xinjiang region. More than a million people are reported to be suffering from arbitrary detention in camps, physical torture and pervasive surveillance which aims to forcefully assimilate them as ethnic Chinese. The global community should not only condemn but also sanction these appalling deliberate actions. The utilisation of cutting-edge technology for profiling and surveillance purposes in Xinjiang is the global showcase for how this technology can be abused to an inconceivable degree.

2. Serious consideration should be given to the growing cyber-threats to European citizens which derive from Chinese digital authoritarianism and its spillovers. EU member states and supranational institutions have to strengthen the necessary legal framework and response mechanisms to protect Europeans from cyber-attacks, compromised online privacy and vulnerable personal devices, as well as illicit tracking and surveillance. The mass market penetration of affordable, Chinese-made interconnected IoT devices may be beneficial for European users but also carries potential vulnerabilities. The EU must better engage with China to improve technological standards and ensure rigorous safety checks.

3. The Chinese Social Credit System, though still in its infancy, could have serious implications for the operations of European businesses in China. The EU should be prepared to use counter-measures to shield and support its companies against discriminatory measures. European diplomacy must also anticipate the extension of the system to European nationals residing in China.

4. The new European Commission should follow up on its commitment to set comprehensive European standards for AI. Such a framework must go beyond ethical provisions, setting binding rules and establishing strict red lines when it comes to advanced technology. What safeguards should be in place for facial-recognition software? Which specific requirements should be adopted to ensure the transparency and accountability of automated decision-making

algorithms? National and European institutions should provide a clear set of rules and be ready to block third-country technological imports which do not meet European standards.

5. A strategic goal for the EU is to strengthen its Digital Single Market through better synchronising the regulatory frameworks of its member states—the current situation remains far from ideal. European entrepreneurs, digital businesses and start-up companies are placed at a disadvantage which prevents them from fully tapping into the huge European market. The digital rise of China can be seen as a threat, but it can also provide numerous opportunities for improved cooperation and enhanced trade. However, only a strong and prosperous European Digital Single Market can protect its interests globally, ensure positive reciprocal relationships and even exert pressure when necessary.

6. A collective response is key. The Union has to adhere to its name and strategic purpose and present a united front against the challenges of digital authoritarianism. The EU must ensure internal cohesiveness and make sure that Chinese bilateral or regional trade efforts do not break European unity or influence the EU's foreign policy. A common approach to addressing cybersecurity risks relating to the future 5G network roll-out or cyber-espionage is essential. Additionally, a strengthened mechanism for the screening of foreign direct investment from third countries should be at the disposal of the European Commission in order to mitigate potential security risks and interference in domestic matters.

7. The EU should commit increased resources and political attention to providing attractive international partnerships which can compete with the Chinese BRI. Efforts such as the current EU–Asia Connectivity platform and the enhanced partnership with Japan in the field of digital services, transportation and energy should be strengthened and fully expanded to other countries in the region. Similar ambitious and transparent initiatives should be urgently developed and implemented in Africa with partner countries.

8. The EU should increase cooperation with the US in setting up a comprehensive strategy to contain digital authoritarianism. The long-term digital threats from actors such as China and Russia or their proxies threaten the citizens and the interests of the transatlantic community. In its 2019 London Declaration, NATO emphasised the need to ensure the security of

communications, including 5G technology, as well as recognising China's growing influence as both an opportunity and a challenge. The North Atlantic alliance should remain committed to effective deterrence tactics in the cyber domain.

9. EU member states continue to export specific items, software and advanced technologies which have dual civilian and military applications. Third countries and authoritarian regimes such as China can exploit these technologies for mass surveillance, military purposes and even for the proliferation of weapons of mass destruction. The European Parliament and Council must make use of the ongoing update of the review of dual-use export controls to minimise Europe's contribution to the Chinese development of technology which egregiously abuses human rights internally and internationally.

10. Europe should address the widening gap in its knowledge and understanding of Chinese politics, language and society. European politicians, journalists and policy experts are placed at a disadvantage given the opacity and complexity of Chinese institutions, the ruling CPC and societal trends. The EU should directly fund independent research, language understanding and cultural institutes to help overcome this huge gap and enhance European soft power vis-à-vis China.

11. The EU must evaluate its relationship with the third-country technology companies, especially social media platforms, that are responsible for the exploitation of personal data, the behavioural profiling of users and the spread of damaging disinformation. The European Commission must develop clear rules regarding online platform liability; better implement Europe-wide provisions for ensuring the protection of personal data and private communication; and, where necessary, rely on its tools for the enforcement of competition law.

Bibliography

Allen-Ebrahimian, B., 'Exposed: China's Operating Manuals for Mass Internment and Arrest by Algorithm', China Cables, International Consortium of Investigative Journalists (24 November 2019), accessed at https://www.icij.org/investigations/china-cables/exposed-chinas-operating-manuals-for-mass-internment-and-arrest-by-algorithm/ on 27 November 2019.

Ash, A., '"1984" Algorithm to Control Life in China', *The Times*, 11 June 2017, accessed at https://www.thetimes.co.uk/article/china-introduces-social-credit-system-to-rate-citizen-behaviour-bksgrgzqh on 22 November 2019.

Atkinson, R., speech made at a discussion on 'The Role of Technology in the US–China Trade War', organised by the Brookings Institution, Washington, DC, 18 July 2019, accessed at https://www.brookings.edu/wp-content/uploads/2019/07/global_20190718_china_tech_trade_transcript.pdf on 10 December 2019.

Balding, C. and Clarke, D., *Who Owns Huawei?*, SSRN Scholarly Paper (17 April 2019), accessed at https://papers.ssrn.com/abstract=3372669 on 21 November 2019.

Bandurski, D., 'Lu Wei: The Internet Must Have Brakes', *China Media Monitor*, 11 September 2014, accessed at https://chinamediaproject.org/2014/09/11/lu-wei-the-internet-must-have-brakes/ on 21 November 2019.

Bank for International Settlements, *BigTech and the Changing Structure of Financial Intermediation*, BIS Working Papers no. 779 (April 2019), accessed at https://www.bis.org/publ/work779.pdf on 22 November 2019.

BBC News, 'China Due to Introduce Face Scans for Mobile Users', 1 December 2019, accessed at https://www.bbc.com/news/world-asia-china-50587098 on 11 December 2019.

BBC News, 'China Employs Two Million Microblog Monitors State Media Say', 4 October 2013, accessed at https://www.bbc.com/news/world-asia-china-24396957 on 21 November 2019.

Berwick, A., 'How ZTE Helps Venezuela Create China-Style Social Control', Reuters Special Report (14 November 2018), accessed at https://www.reuters.com/investigates/special-report/venezuela-zte/ on 22 November 2019.

Berwick, A., 'Service? Don't Rely on Venezuela's State Telecoms Firm Cantv', *Reuters*, 23 November 2018, accessed at https://www.reuters.com/article/us-venezuela-cantv/service-dont-rely-on-venezuelas-state-telecoms-firm-cantv-idUSKCN1NR1GQ on 22 November 2019.

Bischoff, P., 'The World's Most-Surveilled Cities', *Comparitech* (15 August 2019), accessed at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ on 21 November 2019.

Boddy, S. and Shattuck, J., *Threat Analysis Report: The Hunt for IOT – The Growth and Evolution of Thingbots Ensure Chaos*, F5 Labs (March 2018), accessed at https://www.f5.com/content/dam/f5/f5-labs/articles/20180313_iot_vol4/F5_Labs_Hunt_for_IOT_Vol_4_rev30MAR18.pdf on 10 December 2019.

Buolamwini, J. and Gebru T., 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research* 81 (2018), 1–15.

Campbell, C., 'China Says It's Building the New Silk Road. Here Are Five Things to Know Ahead of a Key Summit', *Time*, 12 May 2017, accessed at https://time.com/4776845/china-xi-jinping-belt-road-initiative-obor/ on 22 November 2019.

Carnegie Endowment for International Peace, *AI Global Surveillance Index* (2019), accessed at https://carnegieendowment.org/publications/interactive/ai-surveillance on 10 December 2019.

Cave, D. et al., *Mapping China's Tech Giants*, Australian Strategic Policy Institute (18 April 2019), accessed at https://www.aspi.org.au/report/mapping-chinas-tech-giants on 21 November 2019.

Centre for Strategic and International Studies, 'Significant Cyber Incidents' (2019), accessed at https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents on 10 December 2019.

Charlton, E., 'Most People on the Internet Live in This Country', World Economic Forum (27 June 2019), accessed https://www.weforum.org/agenda/2019/06/most-people-on-the-internet-live-in-this-country/ on 21 November 2019.

China Daily Asia, 'Xi Slams "Double Standards" in Cyberspace', 16 December 2015, accessed at https://www.chinadailyasia.com/nation/2015-12/16/content_15359450.html on 21 November 2019.

China Power, 'How Will the Belt and Road Initiative Advance China's Interests?' Center for Strategic and International Studies (8 May 2017), accessed at https://chinapower.csis.org/china-belt-and-road-initiative/ on 22 November 2019.

Creemers, R. et al., 'China's Cyberspace Authorities Set to Gain Clout in Reorganization', *New America*, 26 March 2018, accessed at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/ on 21 November 2019.

Creemers, R., *China's Social Credit System: An Evolving Practice of Control*, SSRN (9 May 2019), accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 on 22 November 2019.

Creemers, R., 'Some Regulations Concerning Publishing Name List Information of Persons Subject to Enforcement for Trust-Breaking', *China Copyright and Media*, 8 November 2016, accessed at https://chinacopyrightandmedia.wordpress.com/2013/07/16/some-regulations-concerning-publishing-name-list-information-of-persons-subject-to-enforcement-for-trust-breaking/ on 22 November 2019.

Daum, J., 'China Through a Glass, Darkly', *China Law Translate*, 24 December 2017, accessed at https://www.chinalawtranslate.com/seeing-chinese-social-credit-through-a-glass-darkly/?lang=en on 22 November 2019.

Daum, J., 'Getting Rongcheng Right', *China Law Translate*, 29 March 2019, accessed at https://www.chinalawtranslate.com/en/getting-rongcheng-right/ on 22 November 2019.

Daum, J., 'Social Credit Overview Podcast', *China Law Translate*, 31 October 2018, accessed at https://www.chinalawtranslate.com/en/social-credit-overview-podcast/ on 21 November 2019.

Dockrill, P., 'China's Chilling "Social Credit System" Is Straight out of Dystopian Sci-Fi, and It's Already Switched on', *Science Alert*, 20 September 2018, accessed at https://www.sciencealert.com/china-s-dystopian-social-credit-system-science-fiction-black-mirror-mass-surveillance-digital-dictatorship on 22 November 2019.

El Kadi, T. H., 'The Promise and Peril of the Digital Silk Road', Chatham House, The Royal Institute of International Affairs (6 June 2019), accessed at https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road on 22 November 2019.

EU Chamber of Commerce in China and Sinolytics, *The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors* (August 2019), accessed at https://www.sinolytics.de/wp-content/uploads/2019/08/Sinolytics_The-Digital-Hand-How-Chinas-Corporate-Social-Credit-System-Conditons-Market-Actors.pdf on 22 November 2019.

European Commission, *EU–China—A Strategic Outlook*, Communication, JOIN (2019) 5 final (12 March 2019), accessed at https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf on 21 November 2019.

EY, *Global FinTech Adoption Index 2019* (June 2019), accessed at https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf on 22 November 2019.

Fan, W. et al., 'China Snares Innocent and Guilty Alike to Build World's Biggest DNA Database', *The Wall Street Journal*, 26 December 2017, accessed at https://www.wsj.com/articles/china-snares-innocent-and-guilty-alike-to-build-worlds-biggest-dna-database-1514310353 on 21 November 2019.

Feldstein, S., *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace (September 2019), accessed at https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final.pdf on 22 November 2019.

Haide, D. et al., 'EU Ambassadors Band Together Against Silk Road', *Handelsblatt Today*, 17 April 2018, accessed at https://www.handelsblatt.com/today/politics/china-first-eu-ambassadors-band-together-against-silk-road/23581860.html?ticket=ST-8704873-idWihnF2hpjTzchnUk1I-ap2 on 22 November 2019.

Hancock, T. and Yizhen J., 'China Pays Record $22bn in Corporate Subsidies in 2018', *Financial Times*, 27 May 2019, accessed at https://www.ft.com/content/e2916586-8048-11e9- b592-5fe435b57a3b on 21 November 2019.

Harding, B., 'China's Digital Silk Road and Southeast Asia', Center for Strategic and International Studies (15 February 2019), accessed at https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia on 22 November 2019.

Hawkins, A. 'Beijing's Big Brother Tech Needs African Faces', *Foreign Policy*, 24 July 2018, accessed at https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ on 5 December 2019.

Hillman, J. E. and McCalpin, M., 'Watching Huawei's "Safe Cities"', Center for Strategic and International Studies, CSIS Briefs (4 November 2019) accessed at https://www.csis.org/analysis/watching-huaweis-safe-cities on 22 November 2019.

Hodge, N. and Ilyshina, M., 'Putin Signs Law to Create an Independent Russian Internet', *CNN*, 1 May 2019, accessed at https://edition.cnn.com/2019/05/01/europe/vladimir-putin-russian-independent-internet-intl/index.html on 21 November 2019.

Hoffman, S., *Social Credit Technology—Enhanced Authoritarian Control With Global Consequences,* Australian Strategic Policy Institute, Report no. 06/2018 (June 2018), accessed at https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-06/Social%20credit_1.pdf?O3X2xnkGONvJFjK4Z57Xbf06lget_MID on 22 November 2019.

Hookway, J., 'Vietnam Tightens Grip on Internet With Data-Storage Law', *The Wall Street Journal*, 12 June 2018, accessed at https://www.wsj.com/articles/vietnam-tightens-grip-on-internet-with-data-storage-law-1528799753 on 21 November 2019.

Horn, S. et al., *China's Overseas Lending*, The National Bureau of Economic Research, Working Paper 26050 (July 2019), accessed at https://www.nber.org/papers/w26050 on 22 November 2019.

Huawei, 'Huawei Creates a Smart City Nervous System for More Than 100 Cities With Leading New ICT', Press release (14 November 2017), accessed at https://www.huawei.com/en/press-events/news/2017/11/Huawei-Smart-City-Nervous-System-SCEWC2017 on 22 November 2019.

Human Rights Watch, 'UN: Unprecedented Joint Call for China to End Xinjiang Abuses' (10 July 2019), accessed at https://www.hrw.org/news/2019/07/10/un-unprecedented-joint-call-china-end-xinjiang-abuses on 27 November 2019.

IMF, 'People's Republic of China', Country Report no. 18/240 (July 2018) accessed at https://www.imf.org/en/Publications/CR/Issues/2019/08/08/Peoples-Republic-of-China-2019-Article-IV-Consultation-

Press-Release-Staff-Report-Staff-48576 on 10 December 2019.

IMF, 'People's Republic of China', Country Report no. 19/274 (August 2019), accessed at https://www.imf.org/~/media/Files/Publications/CR/2019/1CHNEA2019004.ashx on 21 November 2019.

Inskter, N., *China's Cyber Power* (London: Routledge, 1st edition, 2016).

Kennedy, S. and Rosen, D., 'Market Metrics: A Fact-Based Approach to the Chinese Economic Challenge', Center for Strategic and International Studies (10 October 2019), accessed at https://www.csis.org/analysis/market-metrics-fact-based-approach-chinese-economic-challenge on 21 November 2019.

Kharas, H., *The Unprecedented Expansion of the Global Middle Class: An Update*, Brookings Institution (February 2017), accessed at https://www.brookings.edu/wp-content/uploads/2017/02/global_20170228_global-middle-class.pdf on 22 November 2019.

Kharpal, A., 'China Wants to Be a $150 Billion World Leader in AI in Less Than 15 Years', *CNBC*, 21 July 2019, accessed at https://www.cnbc.com/2017/07/21/china-ai-world-leader-by-2030.html on 22 November 2019.

King, G. et al., 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', *American Political Science Review* 111/3 (2017), 484–501, accessed at https://gking.harvard.edu/50c on 22 November 2019.

Koleski, K. and Salidjanova, N., *China's Technonationalism Toolbox: A Primer*, US–China Economic and Security Review Commission (28 March 2018), accessed at https://www.uscc.gov/sites/default/files/Research/China%27s%20Technonationalism.pdf on 21 November 2019.

Kolton, M., 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence', *The Cyber Defence Review* 2/1 (2017), 119–53, accessed at https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Interpreting%20Chinas%20Pursuit%20of%20Cyber%20Sovereignty_Kolton.pdf?ver=2018-07-31-093726-797 on 21 November 2019.

Kostka, G., *China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval,* SSRN (23 July 2018), accessed at https://ssrn.com/abstract=3215138 on 22 November 2019.

Kuo, L., 'China Bans 23m From Buying Travel Tickets as Part of "Social Credit" System', *The Guardian*, 1 March 2019, accessed at https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system on 22 November 2019.

Lewis, J. A., *China's Pursuit of Semiconductor Independence*, Center for Strategic and International Studies (January 2019), accessed at https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence on 21 November 2019.

Liu, J. and Xiqing, W., 'In Your Face: China's All-Seeing State', *BBC News*, 10 December 2017, accessed at https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state on 21 November 2019.

Maçães, B., *China's Belt and Road: Destination Europe*, Carnegie Europe (9 November 2016), accessed at https://carnegieendowment.org/files/Maes_Chinas_Belt_and_Road.pdf on 22 November 2019.

Maizland, L., 'China's Repression of Uighurs in Xinjiang', Council on Foreign Relations (25 November 2019), accessed at https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang on 27 November 2019.

Martina, M., 'Business Group Issues Wake-up Call on China's Corporate "Social Credit" Plan', *Reuters*, 28 August 2019, accessed at https://www.reuters.com/article/us-china-eu-business-socialcredit/business-group-issues-wake-up-call-on-chinas-corporate-social-credit-plan-idUSKCN1VI037 on 22 November 2019.

Martina, M., 'Exclusive: In China, the Party's Push for Influence Inside Foreign Firms Stirs Fears', *Reuters*, 24 August 2017, accessed at https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU on 21 November 2019.

Masters, J., 'What Is Internet Governance?', Council on Foreign Relations (23 April 2014), accessed at https://www.cfr.org/backgrounder/what-internet-governance on 21 November 2019.

Matsakis, L., 'How the West Got China's Social Credit System Wrong', *Wired*, 29 July 2019, accessed at https://www.wired.com/story/china-social-credit-score-system/ on 22 November 2019.

McBride, J. and Chatzky, A., 'Is "Made in China 2025" a Threat to Global Trade?', Council on Foreign Relations (2019), accessed at https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade on 21 November 2019.

McCarthy, N., '1.7 Billion Adults Worldwide Do Not Have Access to a Bank Account', *Forbes*, 8 June 2018, accessed at https://www.forbes.com/sites/niallmccarthy/2018/06/08/1-7-billion-adults-worldwide-do-not-have-access-to-a-bank-account-infographic/#6ba9aae84b01 on 21 November 2019.

Meissner, M., *China's Social Credit System: A Big-Data Enabled Approach to Market Regulation With Broad Implications for Doing Business in China*, Mercator Institute for China Studies (24 May 2017), accessed at https://www.merics.org/sites/default/files/2018-05/merics_ChinaMonitor_39_englisch_Web.pdf on 22 November 2019.

Mitchell, A. and Diamond, L., 'China's Surveillance State Should Scare Everyone', *The Atlantic*, 2 February 2018, accessed at https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ on 22 November 2019.

Mozuer, P. et al., 'Made in China, Exported to the World: The Surveillance State', T*he New York Times*, 24 April 2019, accessed at https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html on 22 November 2019.

Nebehay, S., 'U.N. Says It Has Credible Reports That China Holds Million Uighurs in Secret Camps', *Reuters*, 10 August 2018, accessed at https://www.reuters.com/article/us-china-rights-un-idUSKBN1KV1SU on 27 November 2019.

Nichols, M., 'Saudi Arabia Defends Letter Backing China's Xinjiang Policy', *Reuters*, 19 July 2019, accessed at https://www.reuters.com/article/us-china-rights-saudi/saudi-arabia-defends-letter-backing-chinas-xinjiang-policy-idUSKCN1UD36J on 9 December 2019.

Ohlberg, M. et al., *Central Planning, Local Experiments The Complex Implementation of China's Social Credit System*, Mercator Institute for China Studies (12 December 2017), accessed at https://www.merics.org/sites/default/files/2018-03/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf on 22 November 2019.

Osborne, H. and Cutler, S., 'Chinese Border Guards Put Secret Surveillance App on Tourists' Phones', *The Guardian*, 2 July 2019, accessed at https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones on 10 December 2019.

Parkinson, J. et al., 'Huawei Technicians Helped African Governments Spy on Political Opponents', *The Wall Street Journal*, 15 August 2019, accessed at https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 on 10 December 2019.

Prasso, S., 'China's Digital Silk Road is Looking More Like an Iron Curtain', *Bloomberg*, 10 January 2019, accessed at https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain on 22 November 2019.

Quiang, X., 'The Road to Digital Unfreedom: President Xi's Surveillance State', *Journal of Democracy* 30/1 (2019), 53–67, accessed at https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/#f6 on 10 December 2019.

Radio Free Liberty, 'Putin Signs "Sovereign Internet" Law, Expanding Government Control of Internet' (1 May 2019), accessed at https://www.rferl.org/a/putin-signs-sovereign-internet-law-expanding-government-control-of-internet/29915008.html on 22 November 2019.

Rogin, J., 'White House Calls China's Threats to Airlines "Orwellian Nonsense"', *Washington Post*, 5 May 2018, accessed at https://www.washingtonpost.com/news/josh-rogin/wp/2018/05/05/white-house-calls-chinas-threats-to-airlines-orwellian-nonsense/ on 22 November 2019.

Rollet, C., 'China Public Video Surveillance Guide: From Skynet to Sharp Eyes', IPVM (14 June 2018), accessed at https://ipvm.com/reports/sharpeyes on 21 November 2019.

Ryan F. et al., 'Mapping More of China's Technology Giants', Australian Strategic Policy Institute, Report no. 24/29 (November 2019), accessed at https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-11/Mapping%20more%20of%20Chinas%20tech%20giants_1.pdf?cONTm6ETA8RMzlcILgDFNdoHdMN6xGZf on 10 December 2019.

Segal, A., 'When China Rules the Web', *Foreign Affairs*, September/October 2018, accessed at https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web on 21 November 2019.

Shahbaz, A., *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (October 2018), accessed at https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf on 22 November 2019.

Shi-Kupfer, K. and Ohlberg, M., *China's Digital Rise: Challenges for Europe*, Papers on China no. 7, Mercator Institute for China Studies (April 2019), accessed at https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_final.pdf on 21 November 2019.

Shi-Kupfer, K. and Ohlberg, M., 'The Party Does Not Yet Rule Over Everything', Mercator Institute for China Studies (29 November 2018), accessed at https://www.merics.org/en/china-monitor/the-party-does-not-yet-rule-over-everything on 21 November 2019.

Simonite, T., 'Behind the Rise of China's Facial-Recognition Giants', *Wired*, 9 March 2019, accessed at https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/# on 21 November 2019.

Síthigh, D. and Siems, M., *The Chinese Social Credit System: A Model for Other Countries?*, European University Institute Working Papers, LAW 2019/01 (January 2019), accessed at https://cadmus.eui.eu/bitstream/handle/1814/60424/LAW_2019_01.pdf?sequence=1 on 10 December 2019.

Stecklow, S. et al., 'U.S. Ban on Sales to China's ZTE Opens Fresh Front as Tensions Escalate', *Reuters*, 16 April 2018, accessed at https://www.reuters.com/article/us-china-zte/u-s-ban-on-sales-to-chinas-zte-opens-fresh-front-as-tensions-escalate-idUSKBN1HN1P1 on 21 November 2019.

Tao, H., 'Zhima Credit Does Not Share User Scores or Data', *Financial Times*, 15 November 2017, accessed at https://www.ft.com/content/ec4a2a46-c577-11e7-a1d2-6786f39ef675 on 21 November 2019.

The Hudson Institute, 'Remarks by Vice President Pence on the Administration's Policy Toward China' (4 October 2018), accessed at https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/ on 22 November 2019.

Tilouine, J. and Kadiri, G., 'A Addis-Abeba, le siège de l'Union africaine espionné par Pékin', *Le Monde*, 26 January 2018, accessed at https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html on 22 November 2019.

Turkey, Ministry of Foreign Affairs, 'Statement of the Spokesperson of the Ministry of Foreign Affairs, Mr. Hami Aksoy', QA-6 (9 February 2019), accessed at http://www.mfa.gov.tr/sc_-06_-uygur-turklerine-yonelik-agir-insan-haklari-ihlalleri-ve-abdurrehim-heyit-in-vefati-hk.en.mfa on 27 November 2019.

US, Bureau of Industry and Security Commerce, *Addition of Certain Entities to the Entity List*, Federal Register (10 September 2019), accessed at https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list on 22 November 2019.

US Chamber of Commerce, 'Competing Interests in China's Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy' (9 August 2014), accessed at https://www.uschamber.com/sites/default/files/aml_final_090814_final_locked.pdf on 21 November 2019.

US–China Economic and Security Review Commission, *2017 Annual Report to Congress* (2017), accessed at https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%204%2C%20Section%201%20-%20China%27s%20Pursuit%20of%20Dominance%20in%20Computing%2C%20Robotics%2C%20and%20Biotechnology.pdf on 21 November 2019.

von Blomberg, M., 'The Social Credit System and China's Rule of Law', *Mapping China Journal* 2 (2017), 77–162, accessed at https://mappingchina.org/wp-content/uploads/2019/01/MCJ-No-2-2018-Blomberg.pdf on 22 November 2019.

Wang, M., 'China's Chilling "Social Credit" Blacklist', Human Rights Watch (12 December 2017), accessed at https://www.hrw.org/news/2017/12/12/chinas-chilling-social-credit-blacklist on 22 November 2019.

Wei, L., 'Cyber Sovereignty Must Rule Global Internet', *Huffpost*, 15 December 2014, accessed at https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060 on 10 December 2019.

Wenyan, W., 'China Is Waking up to Data Protection and Privacy. Here's Why That Matters', World Economic Forum (12 November 2019) accessed at https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline on 10 December 2019.

Williams, S., 'Attacks on IoT Devices Booming, Research Finds', *SecurityBrief*, 24 October 2019, accessed at https://securitybrief.eu/story/attacks-on-iot-devices-booming-research-finds on 10 December 2019.

Wong, S. and Martina, M., 'China Adopts Cyber Security Law in Face of Overseas Opposition', *Reuters*, 7 November 2016, accessed at www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049 on 21 November 2019.

Yuan, L., 'A Generation Grows up in China Without Google, Facebook or Twitter', *The New York Times*, 6 August 2018, accessed at https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html on 21 November 2019.

Zenglein, M. J. and Holzmann, A., *Evolving Made in China 2025*, Papers on China no. 8, Mercator Institute for China Studies (July 2019), accessed at https://www.merics.org/sites/default/files/2019-07/MPOC_8_MadeinChina_2025_final_3.pdf on 21 November 2019.

Zenz, A., *China's Domestic Security Spending: An Analysis of Available Data*, The Jamestown Foundation, China Brief 18/4 (12 March 2018), accessed at https://jamestown.org/program/chinas-domestic-security-spending-analysis-available-data/ on 21 November 2019.

Digital authoritarianism is no future prospect. It is already here. The People's Republic of China has institutionalised draconian measures for citizen surveillance and censorship, as well as gaining almost full control of online political discourse. The Chinese Social Credit System is an intricate extension of this tactic. A coordinated administrative system which feeds on data from different governmental sources and has the ability to sanction and publicly shame individuals would be a powerful tool in the hands of the Chinese Politburo. In parallel, China is pursuing an aggressive agenda of techno-nationalism which aims to move the country closer to technological self-sufficiency and to maximise the penetration of its technological giants on the global stage. The majority of these digital champions have been nurtured by generous public subsidies and successfully shielded from international competition.

This research paper analyses the unique features of the Chinese model of digital authoritarianism and its international spill-overs. China's oppressive model is no longer just applied domestically but is successfully being exported to other countries across different continents. A comprehensive European strategy is needed to withstand the direct threat to the EU's vital interests and inherent democratic values. As a new decade begins, the EU must make sure that its citizens have the necessary institutional and legal protection from abuses of modern technology such as facial-recognition software and the advanced application of AI. Europe must remain a global influence when it comes to ensuring a coherent regulatory approach to technology and stand ready to oppose the spread of digital authoritarianism.

Wilfried
Martens Centre
for European Studies