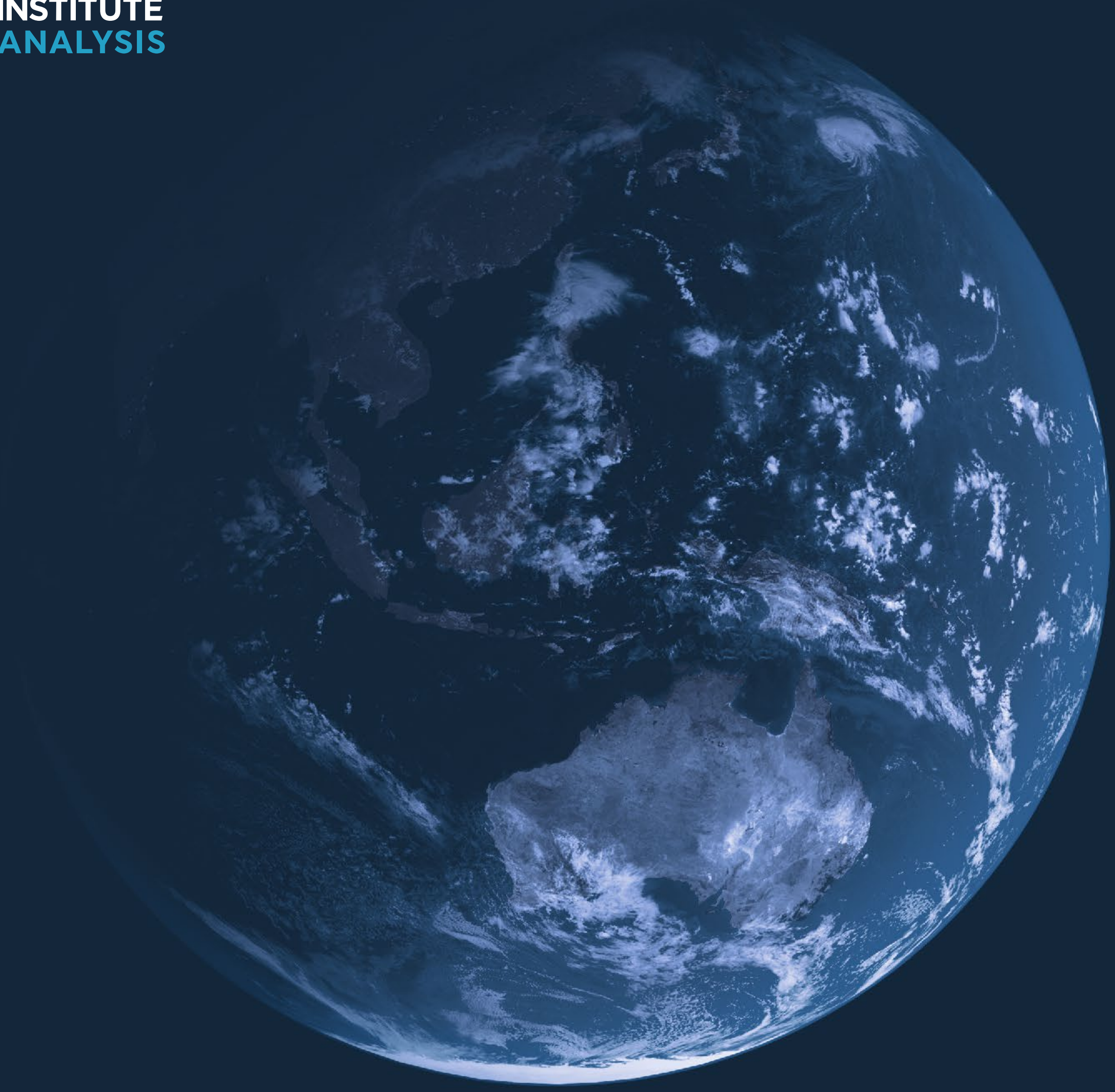
LOWY
INSTITUTE
ANALYSIS



Digital Authoritarianism, China and C0VID

LYDIA KHALIL

NOVEMBER 2020

The Lowy Institute is an independent policy think tank. Its mandate ranges across all the dimensions of international policy debate in Australia — economic, political and strategic — and it is not limited to a particular geographic region. Its two core tasks are to:

- produce distinctive research and fresh policy options for Australia's international policy and to contribute to the wider international debate
- promote discussion of Australia's role in the world by providing an accessible and high-quality forum for discussion of Australian international relations through debates, seminars, lectures, dialogues and conferences.

Lowy Institute Analyses are short papers analysing recent international trends and events and their policy implications.

The views expressed in this paper are entirely the author's own and not those of the Lowy Institute.

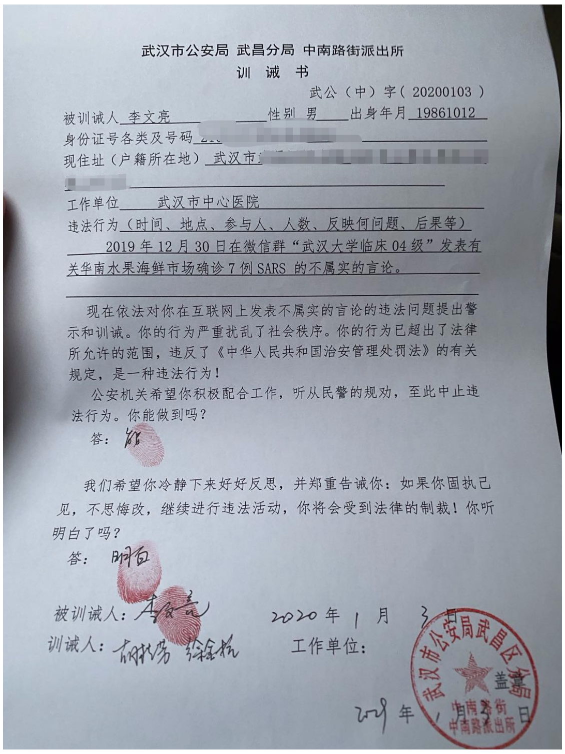
EXECUTIVE SUMMARY

The combination of retreating US leadership and the COVID-19 pandemic has emboldened China to expand and promote its tech-enabled authoritarianism as world's best practice. The pandemic has provided a proof of concept, demonstrating to the CCP that its technology with 'Chinese characteristics' works, and that surveillance on this scale and in an emergency is feasible and effective. With the CCP's digital authoritarianism flourishing at home, Chinese-engineered digital surveillance and tracking systems are now being exported around the globe in line with China's Cyber Superpower Strategy.

China is attempting to set new norms in digital rights, privacy, and data collection, simultaneously suppressing dissent at home and promoting the CCP's geostrategic goals. The danger for other countries importing Chinese technological solutions is that it will result in a growing acceptance of mass surveillance, habituation to restrictions on liberties, and fewer checks on the collection and use of personal data by the state, even after the public health crisis subsides.[1] Democratic governments need to be vigilant in setting standards and preserving citizens' rights and liberties.

INTRODUCTION

In April 2020 Dr Ai Fen, head of the emergency department at Wuhan Central Hospital, gave an interview to Chinese magazine *Renwu*.[2] She described in great detail how, late in December 2019, she had begun receiving numerous patients into the emergency room with flu-like symptoms that were resistant to the usual treatments. She recounted how she "broke out in a cold sweat" when the first virus report of one of those patients came back. She hastily circled the words "SARS coronavirus", screen-shot the report, and sent it to colleagues. Very quickly, her report circulated around Wuhan medical circles. But instead of mobilising the hospital and authorities, Dr Ai's actions saw her reprimanded by the hospital disciplinary committee for "spreading rumours" and "harming stability".[3] Rather than warning staff and the public, hospital authorities told staff not to wear personal protective equipment and relayed instructions from the local health protection committee that, to avoid causing panic, doctors were prohibited from sharing messages and reports related to the virus.[4]



武汉市公安局 武昌分局 中南路街派出所

训 诫 书

武公（中）字（ 20200103 ）

被训诫人 李文亮 性别 男 出身年月 19861012

身份证号各类及号码 [redacted]

现住址（户籍所在地） 武汉市[redacted]

工作单位 武汉市中心医院

违法行为（时间、地点、参与人、人数、反映何问题、后果等）

2019 年 12 月 30 日在微信群"武汉大学临床 04 级"发表有关华南水果海鲜市场确诊 7 例 SARS 的不属实的言论。

现在依法对你在互联网上发表不属实的言论的违法问题提出警示和训诫。你的行为严重扰乱了社会秩序。你的行为已超出了法律所允许的范围，违反了《中华人民共和国治安管理处罚法》的有关规定，是一种违法行为！

公安机关希望你积极配合工作，听从民警的规劝，至此中止违法行为。你能做到吗？

答：能

我们希望你冷静下来好好反思，并郑重告诫你：如果你固执己见，不思悔改，继续进行违法活动，你将会受到法律的制裁！你听明白了吗？

答：明白

被训诫人：李文亮 2020 年 1 月 3 日

训诫人： 工作单位：

武汉市公安局武昌区分局 中南路街派出所 盖章

2019 年 1 月 3 日

Dr Li Wenliang, whose private post regarding coronavirus went viral on social media, was forced to sign a letter of admonition issued by Wuhan police in which he admitted to severely disturbing "social order". Dr Li later died of COVID-19. Image: Wikimedia Commons.

Dr Li’s death sparked outrage in China and was accompanied by calls for greater freedom of expression, government accountability, and opposition to online censorship. Thousands of posts on messaging app WeChat and micro-blogging platform Weibo mourning the death and criticising authorities were not immediately suppressed by internet censors, echoing brief windows of openness that the Chinese Communist Party (CCP) allowed during previous times of crisis.[5] The storm over Dr Li’s death also prompted China’s National Supervisory Commission to conduct an inquiry into the handling of early reports of the virus and Dr Li’s treatment. The official investigation report exonerated Dr Li, apologised to his family, and concluded that the police handling of his reprimand was inappropriate.[6] Wuhan province-level officials were also removed from their posts.

Dr Li’s death sparked outrage in China and was accompanied by calls for greater freedom of expression, government accountability, and opposition to online censorship.

But the same official investigation warned that “hostile forces with ulterior motives, who tried to stir up trouble, delude people, and instigate public emotions, are doomed to fail”.[7] Censors began to remove internet posts and block trending hashtags #WeWantFreedomOfSpeech and #Wuhan Government Owes Dr Li Wenliang An Apology.[8] With the help of artificial intelligence-powered search engine tools, the same internet police that silenced Dr Li were efficiently dispatched to pursue netizens who had written critically about the Chinese government’s handling of the outbreak and Dr Li’s treatment.[9]

Meanwhile, another doctor from Wuhan Central Hospital, Dr Hu Weifeng, died.[10] And Dr Ai, who originally alerted colleagues to the human transfer, had gone missing after her interview with *Renwu* magazine.[11] Although Dr Ai confirmed in a later interview with Radio Free Asia on 14 April that she was safe, rights groups remain concerned that these reassurances were made under pressure from Chinese authorities.[12] Dr Ai’s interview also disappeared from the Chinese internet, preserved only in alternative language blog posts.[13]

Globally, China has been heavily criticised for suppressing early information on COVID-19's emergence, a decision that almost certainly exacerbated the human and economic costs of the global pandemic.[14] According to one study, the CCP could have prevented a significant proportion of COVID-19 cases had they acted on the first warnings and enacted non-pharmaceutical measures (such as quarantines) weeks earlier than was the case.[15]

Dr Ai Fen, Director of Emergency at Wuhan Central Hospital, went missing after an interview with Renwu magazine in which she discussed a spate of patients presenting with a new strain of SARS/coronavirus. Image: Renwu/handout.

The CCP has reacted to this criticism with further censorship and propaganda both within China and through external diplomatic efforts. For example, within China, the Cyberspace Administration of China (CAC) has forbidden the online circulation of videos or posts criticising police enforcement of quarantine restrictions.[16] Social media posts critical of the CCP's handling of the pandemic are routinely blocked or removed, as are critics' calls for transparency and greater accountability.

This online information suppression increasingly bleeds over into the real world. There are indications that the CCP has escalated its punishment and detention of those who post critically or unfavourably on the government's COVID-19 response or call for greater internet freedoms. The Freedom House China media bulletins have tracked numerous cases of ongoing detention of critics and online censorship since the onset of the pandemic.[17]

But the COVID-19 crisis has done more than generate CCP censorship, information suppression, and manipulation at home. Disinformation campaigns originally aimed at a domestic audience, such as the narrative that the virus originated in the United States rather than

China, leaked out internationally and became part of the CCP’s global propaganda. The pandemic has prompted China to commence what American analyst Laura Rosenberger has dubbed an “information offensive” — a mix of overt and covert operations designed to seed disinformation, discredit other governments’ pandemic responses, and praise China’s domestic response and ‘mask diplomacy’ abroad.[18]

The pandemic has also provided an opening for China to ‘sell’ its model of governance and emergency management abroad.

In part, this is an attempt to quell the global backlash against China’s early mishandling of the outbreak. But the pandemic has also provided an opening for China to ‘sell’ its model of governance and emergency management abroad. China is touting its draconian public health response, including the rapid shutdown of affected provinces, widespread digitised contact tracing, and quarantine enforcement, as a ‘best practice’ model of authoritarian governance. This model was executed via both old-fashioned human-propelled grid management, and through digital technologies, including cutting-edge experimentation with data analytics, digital tracing, and other artificial intelligence (AI) tools.[19]

This Lowy Institute Analysis explores the ways in which China has used the COVID-19 pandemic to expand its model of digital authoritarianism at home, and the degree to which this expansion has helped to export, promote, and normalise the tools of tech-enabled authoritarianism abroad. This is especially important at a time when China is actively pursuing its ambitions for technological dominance, and when a range of governments are curtailing liberties and freedoms and using data collection and surveillance technology in their public health responses to stop the spread of coronavirus. China’s use and export of digital authoritarianism during the COVID-19 era warrants careful analysis, given its far-reaching implications for the rest of the world.[20]

DIGITAL AUTHORITARIANISM EXPLAINED

In essence, digital authoritarianism — also known as tech-enabled authoritarianism — is the use of technology by authoritarian governments not only to control, but to shape, the behaviour of its citizens via surveillance, repression, manipulation, censorship, and the provision of services in order to retain and expand political control. Numerous illiberal or authoritarian governments in East and Central Asia, the Middle East, Africa, and Latin America are using aspects of technology to control their citizens and shore up their regimes. But China and Russia are the main practitioners, and China in particular is spreading its digital authoritarianism model and mechanisms through a combination of technology exports, domestic example-setting, and international engagement.[21]

Digital authoritarianism incorporates tech-enabled incentive and punishment systems, such as China's social credit system.

Identifying, monitoring, and censoring individuals online is the most obvious form of digital authoritarianism. But this is the tip of the iceberg. Digital authoritarianism involves much more than censorship in the online space. It includes individual and mass surveillance through the use of cameras, facial recognition, drones, GPS tracking, and other digital technologies in support of authoritarian governance. It normalises constant surveillance and extinguishes expectations of privacy.

Digital authoritarianism also includes state disinformation campaigns aimed at manipulating citizens, while at the same time punishing and censoring dissenting speech on internet platforms and elsewhere under 'fake news' laws.

In addition to central control over internet governance and infrastructure, digital authoritarians support and co-opt their domestic technology industry to service their efforts to maintain social control and to build state capacity to bolster their legitimacy. Digital authoritarianism incorporates tech-enabled incentive and punishment systems, such as China's social credit system, which institutionalise data transfer between private technology companies and government agencies so as to allow only compliant citizens to participate fully in society and the economy.

Digital authoritarians often adopt the principle of cyber sovereignty — control over the internet within a nation's own borders. This runs counter to the founding principles of the internet, which are net neutrality and the unfettered flow of information. Cyber sovereignty empowers a government to better control the information environment of its citizens, pre-empting the need to censor them.

While digital authoritarianism enables efficient state control and coercion of citizens, it also reduces the necessity to resort to coercion at all. The technology allows for less visible, more automated mechanisms of control and more subtle means of increasing self-censorship, social supervision, and reporting of fellow citizens' behaviour through digital apps. Control of the technology sector also allows for the collection and exploitation of big data, which is fed into algorithms that are developed and used to shape economic and social interactions in ways that advance the values and norms of the governing regimes.[22]

The digital authoritarian technology ecosystem generates massive amounts of data, which the state can then access and analyse in order to shape and control society via surveillance, propaganda, and social credit systems.[23] An adjunct function of the big data gathered by authoritarian regimes is its integration with algorithms to develop AI, not only to monitor individuals' whereabouts and online behaviour, but to map their relationships through link analysis, to discern their intentions or emotions using sentiment analysis, and to infer their past or future locations and actions for the purpose of regime maintenance.[24]

While digital authoritarianism enables efficient state control and coercion of citizens, it also reduces the necessity to resort to coercion at all.

According to the 2019 Freedom House annual "Freedom on the Net" report, there has been a sharp global increase in the abuse of civil liberties and human rights due to the growth of digital authoritarianism.[25] This growth may be driven by China and Russia, but it is also exacerbated by the failure of democratic governments to regulate social media, rein in domestic anti-democratic forces, and take the lead in advocacy for international internet norms and technological standards that promote democratic values.[26] This growing digital authoritarianism not only impairs individual rights and liberties, but also threatens to reshape the power balance between democracies and autocracies globally.[27]

CHINA'S DIGITAL AUTHORITARIAN MODEL

China is the clear leader in tech-enabled autocracy and its model of digital authoritarianism involves the practice of many of the elements described above. The CCP uses technology to achieve social control in ways that are coercive, but also in ways that involve more subtle co-option of individuals and society. The CCP, now under the tightening control of President Xi Jinping, does this without any substantial checks and balances on its power or a civil society free to criticise or hold the government to account.[28]

The CCP uses technology to achieve social control in ways that are coercive, but also in ways that involve more subtle co-option of individuals and society.

The CCP's coercive use of technologies, such as online censorship and mass surveillance, are widely reported. In a recent article in *The Atlantic*, Ross Andersen warned of President Xi's vision to develop China's AI sector in order to create a "digital panopticon" — an "all-seeing digital system of social control, patrolled by precog [future vision] algorithms that identify potential dissenters in real time".[29]

China's model of digital authoritarianism deploys its technology to suppress dissent and manufacture support. But systems and mechanisms for regime maintenance and control that are enabled via technology often piggyback onto otherwise useful tools and services.[30] China also harnesses technology to bring about efficient outcomes for its citizens and to exhibit the superiority of its system, which helps the regime to stave off dissent and bolster patriotic support.[31]

Big Tech

China has invested substantially in building an indigenous technology sector, with accompanying industrial policies, such as the National IT Development Strategy, Made in China 2025, and China Standards 2035. These have furthered the country's goal of becoming a global leader in digital technology and AI, and in the process, positioned China to define global technological standards and to use its tech sector to reinforce regime durability and project the CCP's geostrategic goals.[32]

While China's tech sector is anchored by the big three — Alibaba, Tencent, and Baidu — its start-up culture is ferocious and globally competitive. Even with a dip in venture capital investment in 2019, Chinese technology companies are among the world's largest, most valuable, and most innovative.[33] They are also leaders in research and development, with an ever-expanding global reach and influence.[34] The information transfer between these private companies and government authorities is comprehensive and systematic, and the close links between them leaves companies vulnerable to intense pressure to release data, potentially conferring on the government swift and unfettered access to personal data of increasing intimacy and breadth. Many major tech companies in China have been publicly resistant to releasing such data, but like any company operating in China they can be legally compelled to provide a backdoor for authorities to access any encrypted data.[35] When the CCP can access such information on a broad scale, its big data analytics efforts become more robust and its AI more accurate, with limited protections for privacy or other rights.

Co-founder of e-commerce giant Alibaba, Jack Ma (right), at the IMF/World Bank Group Annual Meeting seminar: Disrupting Development, on 12 October 2018 in Bali, Indonesia. Ma's new Ant Group is set for a record US$34 billion launch on the Shanghai and Hong Kong stock exchanges. Image: Brandon Payne/World Bank.

As Samantha Hoffman, an expert on China’s digital authoritarianism, describes it, “The CCP [has used] technology to make its Gordian knot of political control inseparable from China’s social and economic development.”[36] China imposes the same obligations on technology companies as it does on other large businesses in the country to host party committees and government officials assigned to their operations.[37] Chinese tech companies are also required by law to cooperate in matters of national security and intelligence by way of aiding surveillance and making available their expertise, products, and data for CCP objectives. Although these companies operate on the open market, the CCP has the potential to control “any company at any time”.[38]

Information Control and Censorship

China is known for its 'Great Firewall', in place since the early 2000s. This has allowed China to seal off the Chinese internet from the rest of the world and is a key element of its vision of cyber sovereignty.[39] The Great Firewall's foundation is an interconnected system of laws and regulations that determines acceptable and prohibited content. Bodies such as the Cyberspace Administration of China (CAC) control the internet's infrastructure and content within Chinese borders. The 'bricks' of the Great Firewall include mechanisms such as IP blocking (to bar access to certain content and websites), deep packet inspection (used to examine network traffic), keyword filtering, and banning the use of VPNs (used to gain private access to sites and avoid censorship blocks).[40] Human and artificial censors also filter and remove prohibited content.

Chinese tech companies are leading developers of various monitoring tools to aid in censorship and surveillance. Via popular apps, the government uses these technologies to monitor individuals and block access to services and communication.[41] Unlike Western technology companies, Chinese internet platforms are monitored and controlled by the CAC, which issues licences to internet companies and oversees all internet content. Companies are expected to invest in their own technology and personnel to censor content according to CAC regulations, or face hefty fines or loss of their licences.[42] As a result of vaguely defined guidelines, these platforms have erred on the side of extensive censorship.[43]

Surveillance, Facial Recognition, and Big Data Collection

The mass data the CCP collects on Chinese residents includes online communication, travel logs, records on education and health, facial scans, and bio data. The data is then aggregated and synthesised by AI algorithms to keep 'sharp eyes' on citizens, not only to monitor, but to flag or predict problematic behaviour.

The mass data the CCP collects on Chinese residents includes online communication, travel logs, records on education and health, facial scans, and bio data.

China boasts the world's largest surveillance networks. These are made up of multiple local networks of more than 200 million closed-circuit television (CCTV) cameras in public spaces across the country, outfitted by various companies which provide the data to authorities through programs such as SkyNet, a big-data police video monitoring system.[44] SkyNet collects images at intersections, gathering places, and checkpoints, and maps them using geographic information system

(GIS) mapping to improve real-time monitoring.[45] The program is promoted by the government as a 'smart city' initiative and crime-control mechanism. But it is a constant surveillance presence coupled with facial recognition, crowd analysis, and other AI technology that can be used to monitor citizens and exert all manner of state control.[46]

The success of SkyNet has prompted an even broader surveillance initiative, Sharp Eyes, which aims to link cameras in the 'internet of things' — such as in smartphones, vehicles, televisions, and appliances — with public surveillance cameras. It augments public security infrastructure by encouraging the public to be part of the surveillance system. Implemented initially in rural areas where the CCP's coverage is thinner, Sharp Eyes makes surveillance monitoring even more extensive and precise.[47] The CCP also has plans to use this technology for enhanced logistics and predictive policing applications to aid in state security, anti-terrorism, and criminal activity suppression.[48]

China has made it a national priority to become a global leader in facial recognition and other AI applications.

China has made it a national priority to become a global leader in facial recognition and other AI applications. Chinese tech companies such as Megvii, Yitu, SenseTime, and others are innovators in facial recognition technology, which the CCP leverages to survey its population and project an aura of state omnipotence. Uighurs interned in Xinjiang province have been the first to feel the full weight of the CCP's mass surveillance capabilities, aided by technology provided by companies that specialise in facial recognition and crowd analysis. But the surveillance ambitions extend beyond Xinjiang.[49]

Social Credit Systems

The CCP has placed a high priority on developing and operationalising a national, unified social credit system to build "a Socialist harmonious society".[50] In 2014, the Chinese government issued its Planning Outline for the Construction of a Social Credit System (2014–2020), which laid out a comprehensive national system by establishing a credit record infrastructure network. The stated goal of the system is to promote integrity in individual and social dealings, incentivising 'trustworthy' behaviour and disincentivising behaviour that 'breaks trust'.[51] The system is not fully centralised, and citizens in China do not yet have a national assigned score, as has been frequently reported. Rather, there is a patchwork of individual systems, some run by local governments and others via private company initiatives,[52] particularly in the financial sector, which has its own social credit systems operating alongside those employed by the central government and agencies.

The data collected on China's residents is fed into these systems, some of which have been in place since 2009. The systems rate, reward, or punish citizens, businesses, and government agencies based on their behaviour, and provide a purportedly objective measure of 'trustworthiness'. Points are gained or lost based on behaviour, and the resulting social credit score determines the person's level of access to resources and privileges. Violators are publicly named and shamed. People or companies can be blacklisted for noncompliant behaviour, limiting their access to services and resources for periods of up to three years.[53] Conversely, those with a good score or file are offered preferential treatment in education, travel, housing, employment, medical care, and even access to the internet.

The systems rate, reward, or punish citizens, businesses, and government agencies based on their behaviour, and provide a purportedly objective measure of 'trustworthiness'.

While the ultimate goal of a unified national system has not yet been reached, every citizen in China does have a national credit file, and there are local level social credit systems that do assign scores. But even without a centralised individual number ranking, the national social credit system can still meet its objectives of social control. The National Credit Information Sharing Platform (NCISP), a master database controlled by the central government, is a repository of all social credit systems' data.

Tech companies are being enlisted to develop the NCISP and various social credit scoring systems, as well as dole out rewards and punishments. Many of these companies have signed data-sharing memoranda of understanding (MOUs) with the central government. One of these is Alibaba, which has committed to sharing data and using its platform to issue penalties and rewards.[54] Much of the data used to assess scores of individuals and companies is accessed via these companies' technology, which tracks individuals' actions, interactions, and movements.

Chinese technology companies have also implemented their own social credit systems. Sesame Credit is a private social credit system developed by Ant Financial, an Alibaba subsidiary, which accesses extensive user data from its parent company to help assess scores. To do this, Sesame Credit uses concrete data such as credit history, as well as more abstract measures such as personal characteristics, personal preferences, and interpersonal relationships.[55] The implication is that a credit score can be influenced by the behaviour and score of an individual's personal connections, thus incentivising group- and self-censorship and monitoring. For example, authorities in the Chaoyang District have an arrangement with the makers of the Qihoo 360 app so that users receive notifications when they call or are called by someone on a court blacklist.[56] These private social credit systems are not yet officially part of the government systems, but there are pilot programs in some cities where Alibaba and Tencent are sharing this user data with the expectation that it will be available to the government at some point in the future.[57]

Much of what accounts for trust and integrity, and good and bad behaviour, are defined by the CCP.

While not yet fully integrated, these databases still serve their purpose. And because court judgments are difficult to enforce in China and there have been high profile cases of corruption, parts of the social credit schemes are broadly popular. Yet much of what accounts for trust and integrity, and good and bad behaviour, are defined by the CCP, and there is a high degree of risk that social credit systems can be used not only to sanction illegal conduct, but wielded as an instrument of social control.

Once the centralised national ranking system envisaged in the 2014 Plan is fully realised, the nationwide social credit system will hand the CCP a powerful tool for social management and 'stability' maintenance.[58]

THE IMPACT OF COVID

The CCP's emergency management response to the COVID-19 pandemic has allowed China to expand the use of its digital authoritarian mechanisms at home. Increased tech surveillance and other data collection efforts feed more data into its predictive technologies and AI algorithms, allowing them to develop faster and work better. Surveillance technology in limited use prior to the pandemic was revealed and augmented as part of the CCP's crisis mobilisation.[59] COVID-19 also provided an opportunity for the CCP to showcase the effectiveness of its tech-enabled authoritarian approach abroad, to counter negative perceptions of its inadequate handling of the initial outbreak. With democratic and authoritarian countries alike under unprecedented restrictions and surveillance, the stigma usually associated with such authoritarian measures has been reduced. China has exploited the unusual circumstances to promote its norms and approaches to digital rights, privacy, and data collection, as well as the development and use of AI.

The CCP's emergency management response to the COVID-19 pandemic has allowed China to expand the use of its digital authoritarian mechanisms at home.

Punishment

For decades, China has suppressed dissent within its borders. The coronavirus pandemic has escalated this behaviour in two ways. First, it has given China 'cover' for expanding its already pervasive cyber policing and invasive online surveillance. Second, it has silenced critics and quelled discussion of COVID-19 in the name of virus control, which has also had the added effect of enabling China to more easily exercise 'discourse power'.

According to the database of the Chinese Human Rights Defenders coalition, 897 netizens have been detained, reprimanded, or punished for "spreading rumours", "fabricating false information", "causing panic", "disrupting public/social order", or "leaking privacy" in their online speech related to the COVID-19 outbreak.[60] Those detained included citizen journalists Chen Qiushi, Fang Bin, and Li Zehua, legal advocate Xu Zhiyong, and businessman Ren Zhiqiang. Some, such as former prisoner of conscience Guo Quan and activist Xu Zhiyong, have been detained more than once. In some cases, the detentions were carried out under the guise of mandatory quarantine.[61] Such is the case with legal scholar Xu Zhangrun, who published a critique of the Chinese government's pandemic response and authoritarianism under President Xi.[62] Other intellectuals have been harassed and targeted online for their criticism of the CCP in relation to the pandemic.[63] Still more are held under residential surveillance for their work storing and preserving online content critical of China’s handling of the pandemic that had been deleted or blocked by government censors.[64]

Censorship and Propaganda

The punishments and penalties imposed by Chinese authorities on regime critics have been targeted and draconian, such as on those who criticised the government’s treatment of Dr Li, described earlier. But the CCP’s online censorship has reached far more widely across society. Chinese internet companies are deleting or blocking posts from people who write about family members getting sick, ask for donations or assistance online, or give eyewitness accounts of overwhelming conditions at hospitals.[65] A censorship testing experiment by The Citizen Lab at the University of Toronto found that WeChat and popular livestreaming app YY deleted or blocked posts relating to the virus — not just those critical of the CCP, but also more neutral messages expressing support for medical workers or sympathy for those affected by the pandemic.[66]

This is not the first time the CCP has imposed censorship obligations on Chinese tech companies. But the pandemic context is unique. The early outpouring of grief and anger against Chinese authorities after the initial mishandling and death of Dr Li was widespread. Even prominent party members, academics and business leaders, usually loath to publicly criticise the CCP, speculated about how China's authoritarianism and information suppression had created the conditions for a global pandemic.[67]

State-run media has trumpeted the government's pandemic response, calling it a model for the rest of the world.

Censorship has been even more heavy-handed than usual during the pandemic. In February 2020, the CAC announced that it would punish social media and online platforms for allowing users to publish “harmful” content or for “spreading panic” related to COVID-19. The CAC targeted internet giants Sina Weibo, Tencent, and ByteDance for “special supervision” and management. As a result, other platforms such as WeChat and YY have censored COVID-related posts pre-emptively, interpreting the directive broadly and erasing almost every mention of the virus.

The CCP’s thorough censorship efforts have been complemented by its vigorous propaganda. The central authorities proactively combated criticism of the CCP and its virus response through online disinformation and influence campaigns aimed at its own citizens. State-run media has trumpeted the government's pandemic response, calling it a model for the rest of the world. Memes circulated on the Chinese internet featuring praise for the country from the World Health Organization (WHO). Journalists have been dispatched by authorities to highlight the work of medical staff, all in an effort to vindicate the CCP's pandemic governance model.[68] This combination of censorship and propaganda by state-run media has created an information bubble that serves to insulate Chinese netizens from the outside world. It has prioritised the CCP's narrative within China and left many unaware of growing international criticism of the CCP.[69]

Surveillance, AI, and the Contribution of Chinese Companies

Under pandemic conditions, China's omnipresent digital surveillance system is on full display. Its capacity for surveillance combined with big data analytics has allowed it to automate contact tracing, which makes it effective from a public health perspective. It combines facial recognition technology, security cameras in both public and closed spaces, social media monitoring, telecommunications tracing, and the tracking of digital passenger information. Chinese technology companies are contributing to the data collection via GPS tracking, facial recognition software, and public temperature detection tools. The government couples this with a robust human surveillance network via its grid management system to keep tabs on its citizens, supplementing the human network of local officials with a network of residents to report those suspected of breaching quarantine rules.[70]

A worker adjusts a surveillance camera outside the home of a journalist placed under quarantine in Beijing after he had visited Wuhan, 3 May 2020. Image: Leo Ramirez/AFP via Getty Images.

China's existing digital surveillance programs have been deployed in force to combat the pandemic, and in a manner that has felt more intrusive.

China's existing digital surveillance programs have been deployed in force to combat the pandemic, and in a manner that has felt more intrusive.[71] While surveillance cameras were already ubiquitous in the public square, the health crisis has given Chinese authorities an additional excuse to install cameras outside citizens' front doors or even inside their residences. This is purportedly to enforce quarantines, a move formerly reserved for those who had previously been detained or lived within the Xinjiang region.[72] While not a stated CCP policy, there have been a number of reports of local epidemic control command centres adopting such behaviour.[73] The surveillance camera footage is then linked to police smart phones, flagging quarantine breaches and allowing police to continually monitor living quarters in an increasing invasion of citizens' privacy. One Chinese worker, who like many others must now scan a QR code to enter their own apartment complex and workplace, said, "monitoring is already everywhere. The epidemic has just made that monitoring, which we don't normally see during ordinary times, more obvious".[74]

China has also expanded its surveillance capabilities in other ways. It has deployed thermal temperature scanners and facial recognition technology at transport stations and other public places, using technology and AI from companies such as SenseTime, which claims it is able to identify individuals even when faces are partially obscured with masks.

In response to calls by central authorities for more effective tools for combatting coronavirus outbreaks, other Chinese companies such as Megvii are using AI to integrate body detection, facial recognition, and body temperature.[75] Wearable technology company KC Wearable has developed 'smart helmets' that it claims are able to detect individual temperatures of passers-by, scan QR codes for personal data, and recognise licence plates, as well as identify people using facial recognition software.[76] Through efforts like these, Chinese authorities are able to collect extensive information via the government's 'real name' system that requires government-issued ID to access smartphone SIM cards, sign up for social media accounts, and travel on public transport. Using location tracking and tracing through more than 200 million cameras that employ AI for facial recognition, authorities can now integrate this data with information on personal biometrics.

A number of health code apps have also been developed by tech companies at the behest of provincial government officials. These apps prompt citizens to input their personal information, answer questions related to their exposure to infected people or high-risk areas, and provide travel logs and health status details. They are then assigned a QR code — green/orange/red — based on their calculated infection risk. Anyone without a green code is forbidden from entering stores, stations, or offices that have the system installed. Authorities say the health code apps have helped them ease lockdown restrictions, but provide little transparency on how a colour code is assigned. Some of the tracking apps have reportedly sent data to police. There is no information on how they use that information, nor how or whether the data is stored for future use.[77]

The pandemic, and the imperative to control it, has stalled an emerging public debate on personal data protection.

Contact tracing apps and other tracing technology are not problematic per se. Other countries such as Australia, South Korea, and Taiwan have introduced them.[78] But unlike democracies, when an authoritarian government such as China's uses them on such a broad scale, they are unconstrained by privacy laws, obligations of transparency, public debate, or the ability to hold government to account for any excesses. There is very little publicly available information on the Chinese apps, but they employ an invasive degree of data-mining to extract identities, locations, and even payment histories.[79]

The pandemic, and the imperative to control it, has stalled an emerging public debate on personal data protection.[80] However, the Chinese technology companies that collect the data and provide it to government authorities have amassed huge amounts of their customers' personal information — operating like real-time, privately run digital intelligence gathering agencies. There have been leaks of personal information and reports of surveillance overreach, notwithstanding directives from the CAC on data privacy protection.[81] Despite resistance from the major Chinese tech companies to providing local authorities with consumer data from the multitude of contact tracing apps, the CCP's pressure on those companies has meant that any gains in consumer privacy made over the past couple of years are most probably now lost.[82]

The concern is that the CCP will continue to use these invasive digital technologies after the emergency is over in the name of 'stability' management, much as China continued to expand and consolidate its public CCTV surveillance efforts in the name of security after the Beijing Olympics.[83] As one activist put it:

> *This type of governance and thinking for dealing with the epidemic can also be used for other issues — like the media, citizen journalists or ethnic conflicts. Because this method has been used before, citizens will accept it. It becomes normal.*[84]

Essentially, the pandemic has provided a ‘proof of concept’. It has demonstrated to the CCP and local authorities that the technology works, and that surveillance on this scale and in an emergency is feasible and effective, thus giving the CCP the confidence in its future use. It also reveals to citizens, in China and elsewhere, what is possible, perpetuating self-censorship, normalising tech-enabled monitoring and control, and inducing individuals to embrace, or at least resign themselves to, the overwhelming power of the state.

Expansion of the Social Credit System

The pandemic has also provided ideal conditions for exploiting and adapting the social credit system. Officials who pioneered the health code app are now exploring its other applications, such as ranking citizens with a ‘personal health index’ composed of scores based on sleep, exercise, and smoking and drinking habits.[85] Such a ranking could be integrated into the social credit system to assess suitability for services and jobs, or for monitoring gatherings. This presents a host of opportunities for behaviour management and discrimination. Different local authorities are beginning to adapt the app, linking it to health records, access to other services, and even coupons at local stores, expanding its use for digitised social control.[86]

Essentially, the pandemic has provided a ‘proof of concept’. It has demonstrated to the CCP and local authorities that the technology works, and that surveillance on this scale and in an emergency is feasible and effective.

While local authorities have relaxed some controls during the COVID-19 crisis, such as suspending penalties for late repayment of loans due to financial difficulties, they have incorporated new obligations and created new point scoring incentives. Companies or citizens who make a contribution to the coronavirus effort — such as working in a medical profession or manufacturing medical supplies — are granted points on their social credit score and potentially funnelled into the ‘green channel’, leading to easier administrative access and processing of administrative issues.[87] Conversely, firms engaging in price gouging or selling counterfeit medical products are deducted points, as are individuals who hide their travel or medical information on health apps, refuse medical checks, hoard products, or participate in prohibited large gatherings.[88]

Through these mechanisms, the pandemic has provided an opportunity for Chinese tech companies to harvest and amass significant data with no set limits on how it can be used or how long it can be stored.[89]

Dahua Technology's "Thermal Temperature Monitoring Solution" is capable of identifying individuals with an elevated temperature from a distance of three metres. Image: Dahua Technology handout, LewisSurveillance.com.

There is even talk now in China of establishing a SkyNet-like structure for pre-emptive virus tracking, which would create "an automatic epidemic monitoring and reporting system without any blind spots" using a "combination of new pathogen detection technology and 5G communication, big data and artificial intelligence technology". [90] Prominent biomedical researcher and famed 'virus hunter', Cheng Jing, proposed a system that would change the model of virus tracing from 'passive' reporting to 'active', with automatic and networked tracking via integrated technologies.[91] It is being framed as a means to avoid heavy-handed future lockdown measures such as those imposed in Wuhan after the virus spread.[92] But this would replace stringent physical lockdowns with near constant and ubiquitous surveillance in the name of preventative pandemic measures.

EXPORTING DIGITAL AUTHORITARIANISM ABROAD

Just as the COVID-19 pandemic enabled China to expand surveillance and solidify its digital authoritarian regime at home, it has also provided it with opportunities to export its methods abroad — and criticise and discredit the response of democratic governments, particularly the United States, in the process. The CCP has seized on the current global disarray wrought by the pandemic, the absence of US leadership, and the Trump administration's disorderly pandemic response, as an opportunity to strut on the world stage. Its so-called 'wolf warrior diplomacy' escalated during the pandemic, and it has used vigorous disinformation campaigns to deflect criticism from abroad and tout China as a leader in pandemic response and a global force for good.[93] Early evidence suggests that these techniques may have backfired in many Western democracies, with Pew surveys conducted in mid-2020 showing sharp rises in unfavourable attitudes towards China and President Xi.[94] However, in other countries, including non-democracies that were more favourably disposed to China prior to the pandemic,[95] China's 'mask diplomacy', technology exports, and other overtures may further entrench its strong position, or at least mitigate other negative effects of China's pandemic tactics. As Natasha Kassam noted in *China File* several months into the crisis, "Cambodia, Pakistan, Hungary, and Serbia are praising China's decisive response and expressing gratitude for medical supplies. And while some mask diplomacy has failed due to a lack of quality controls, the real benefits derived in developing countries from receiving teams of medical professionals and webinars in local language shouldn't be underestimated."[96]

China's wolf warrior diplomacy has produced vehement, undiplomatic, and sometimes fantastical attempts to shape its pandemic narrative.

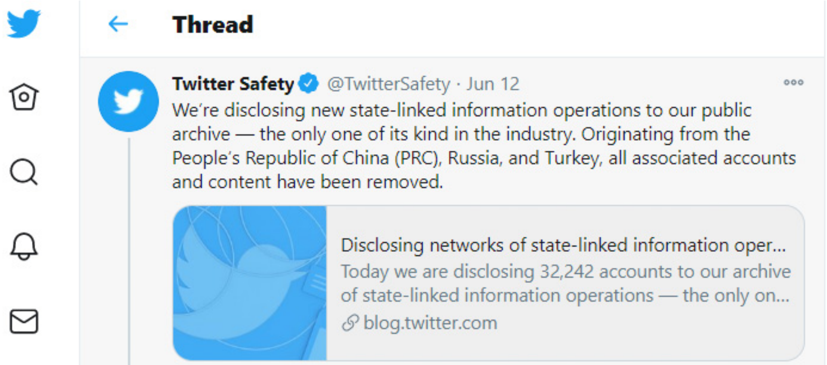
Controlling the Narrative — Wolf Warrior Diplomacy and Disinformation Campaigns

China's wolf warrior diplomacy has produced vehement, undiplomatic, and sometimes fantastical attempts to shape its pandemic narrative.[97] The CCP has wielded its English language tabloid, the *Global Times*, forcefully. For example, a recent opinion piece attempted to deflect criticism of China's pandemic human rights violations claiming that the criticism was:

> *. . . immoral and distorts the truth. Essentially, public health issues are not an issue of human rights. There must be efficient prevention and control . . . When facing the challenge of survival, the rights of individuals must be subordinated to the needs of the majority. This is the same in both Eastern*

and Western ethics. When it comes to life and death, we must first solve the problem of survival before considering how to live more comfortably.[98]

Chinese diplomats, including Chinese deputy head of mission to Australia, Wang Xining, have not only vigorously defended China's handling of the virus, but chastised countries such as Australia for calling for an international investigation into the origins of COVID-19, claiming it "hurt the feelings" of China. Wang was even equivocal in acknowledging that the virus started in Wuhan.[99] This has become a standard talking point of Chinese officials around the world. Other Chinese diplomats have attempted to offer alternative narratives on the origins of the virus, such as foreign ministry spokesman Zhao Lijian, who tweeted conspiracy theories and suggested that US soldiers had brought the virus to Wuhan.[100]



Twitter Safety @TwitterSafety · Jun 12

We're disclosing new state-linked information operations to our public archive — the only one of its kind in the industry. Originating from the People's Republic of China (PRC), Russia, and Turkey, all associated accounts and content have been removed.

Disclosing networks of state-linked information oper...
Today we are disclosing 32,242 accounts to our archive of state-linked information operations — the only on...
blog.twitter.com

Twitter announced its new public "safety" policy, targeting state-linked disinformation campaigns, on 12 June 2020. Twitter has removed more than 150 000 accounts it believes to be spreading Chinese disinformation. Image: Twitter screenshot.

China's disinformation campaigns aimed at international audiences appear to have been highly coordinated. In June, Twitter removed 23 750 undeveloped accounts it assessed were part of an organised effort to praise China's virus response and another 150 000 accounts boosting apparent Chinese disinformation.[101] The European Commission has also accused China of running online disinformation campaigns disparaging Europe's COVID-19 response with the aim of undermining Western democracies.[102]

Technology Exports and the Belt and Road Initiative

Aside from shaping the information environment and attempting to control the narrative on its pandemic response via social media, China is using both passive and active measures to export its tech-enabled surveillance response. Measures once considered extreme among nonauthoritarian governments and societies have become more normalised as the pandemic sweeps across the globe. Through state emergency powers, rights of association and movement have been severely curtailed to curb the virus' spread in democracies and autocracies alike. Pop-up police spy stations track people breaking lockdowns, and students are observed remotely using exam monitoring software.[103] Citizens in democracies have waved away privacy concerns in the interests of public safety, and routinely disclose location, health, and other personal data.

China is not alone in using surveillance and other technology to track and monitor citizens in an effort to contain virus outbreaks.

China is not alone in using surveillance and other technology to track and monitor citizens in an effort to contain virus outbreaks. Israel, Taiwan, India, South Korea, Poland, Australia, and other countries have rolled out COVID-19 tracing or protection apps, and used drones, mobile phone location and financial transaction data to monitor quarantine compliance and track the virus' spread.[104] The virus tracing apps have varying degrees of privacy protections and were rolled out quickly with little testing of their efficacy. The adoption and acceptance of immature technologies such as contact tracing apps and thermal temperature detection cameras by both governments and private companies has been swift. *MIT Technology Review* has compiled an active database of COVID-19 tracing apps from around the world. Of the 47 apps on the list, only 12 countries have introduced systems that meet the full five-star criteria, in that they are voluntary, have limits on how the data is used, require that data is not retained, minimise data collection, and are transparent in design and use.[105]

The pandemic has for most citizens normalised high levels of restriction and surveillance with no indication of when those might abate.[106] Human rights and privacy advocacy organisations have warned that these intrusions into personal liberties and rights may endure, with governments resisting political and social opposition to them even after the public health crisis subsides.[107] At the same time, the public may become inured to more intrusive use of technology, as the world becomes increasingly digitised and automated. There is already a growing acceptance of the narrative promoted by China that privacy and human rights considerations inhibit effective public health responses.[108]

The WHO director-general, Tedros Adhanom Ghebreyesus, has come under scrutiny for stating that “China’s speed, China’s scale and China’s efficiency … is the advantage of China’s system”, without acknowledging the damage caused by China's initial suppression and censorship of information about the virus.[109] Nor does this praise account for the hardships imposed by the severe lockdown measures. Similarly, China's use of "big data and information technology" has been lauded in articles published by bodies such as the World Economic Forum, with little critical evaluation of its effect.[110]

Ya-Qin Zhang, President of tech giant Baidu.com, at the Big Tech, Big Impact session of the Annual Meeting of the World Economic Forum in Davos, 25 January 2018. Image: Sikarin Thanachaiary/World Economic Forum.

Adding to this passive creep of invasive governance, China is using the pandemic to accelerate its export of domestic digital technology, build its dominance in AI and big data, and further the goals defined in the CCP's 2017 Cyber Superpower Strategy. This was first set out in a CCP journal article that outlined the party's strategy for control of China's domestic internet. Apart from encouraging tech-sector investment in AI and other technology breakthroughs, and ensuring the global influence of Chinese tech companies, it sought to promote "China's proposition of internet governance toward becoming an international consensus".[111] President Xi articulated the strategy during the 19th Party Congress in 2017, which included plans to match the United States in AI innovation, quantum computing, and nanotechnology by 2025, and to lead it by 2030.

Even before the 2017 Cyber Superpower Strategy, growth of technology start-ups and AI adoption in China was remarkable. In 2015, the CCP launched Made in China 2025, an industrial policy aimed at expanding China's tech sector and advanced manufacturing capabilities through state subsidies, intellectual property acquisition, and foreign joint ventures.[112] The ultimate goal was to reduce China's dependence on foreign technology and promote Chinese tech manufacturing globally.[113] In the handful of years since the Made in China 2025 and Cyber Superpower Strategy announcements, China has produced dozens of tech unicorns (privately owned start-up companies valued under US$1 billion). It continues its attempts to exert influence over the United Nations International Telecommunication Union regarding surveillance and facial recognition.[114] And this year, it plans to announce its China Standards 2035 blueprint — a vision for influencing future international technology standards and interoperability.[115]

The heavily state-sponsored tech sector serves China's foreign policy and national security strategies.

These strategic documents demonstrate that the CCP's investment in its technology sector is not simply about its own economic development or trade policy.[116] Chinese tech companies and the Chinese tech sector are not acting on market imperatives alone. Despite their protestations, those tech companies are not wholly independent from the Chinese government, as discussed above and as the controversies about Huawei attest.[117] The heavily state-sponsored tech sector serves China's foreign policy and national security strategies. And many of the tech companies are intimately linked to China's intelligence and national security apparatus, while others implicitly understand their acquiescence to the CCP and reliance on heavy subsidies.[118]

In some respects, pandemic and geopolitical considerations such as the ongoing US–China tensions have had a negative impact on the Made in China 2025 strategy. They have reduced the appetites of foreign companies for engaging with China and increased their wariness about forced transfer agreements and other joint venture rules.[119] Yet the pandemic has also allowed the CCP to expand its domestic digital surveillance and AI development and to export this technology as well. In turn, this has promoted Chinese digital authoritarian norms, technology, and AI methods, as tools of political and social control.[120] In other words, technology with 'Chinese characteristics'.

While China has recorded its first economic contraction in decades, its Cyber Superpower Strategy remains on track. The CCP is still investing heavily in 5G technology, surveillance infrastructure, AI, and its tech sector through China's New Infrastructure Investments Fund as part of its post-COVID economic recovery. Through the pandemic, China has positioned itself as a world leader in tech, meeting the technological and security needs of other developing countries.[121] For example, the KC Wearable 'smart helmets' — already in use in parts of China and

Dubai — have been sent to police in Italy and the Netherlands for testing.[122]

Police officers wearing smart helmets stand guard at Chunxi Road on 7 March 2020 in Chengdu, Sichuan Province of China. The smart helmet with an infrared camera can detect body temperature and the result can be displayed in real-time on its screen. Image: Zhang Lang/China News Service via Getty Images.

China is driving global uptake of AI surveillance technology through programs subsidised via the Digital Silk Road (DSR) — the technology component of the Belt and Road Initiative (BRI). This has generated US$17 billion in loans and investments in telecom networks, mobile payment systems, and projects such as smart cities, e-government, smart education, digital health, and other big data initiatives throughout the developing world.[123]

At least 80 countries from Latin America, Africa, and Asia have adopted Huawei's Safe City solutions or other Chinese surveillance and security technology platforms.[124] This excludes other imports and adoptions of other AI technology. Some of the companies importing their technologies are directly state owned (such as China National Electronics Import and Export Corporation, CEIEC). Some have been implicated in human rights violations in Xinjiang, such as Hikvision.[125]

China is supporting its export of technology infrastructure and equipment by offering training on its use and on cyberspace management, and allegedly even assisting other governments to spy on political opponents.[126] In this way, China promotes its digital technology blueprint on AI, surveillance, privacy, rights, and technology's use for 'social stability' abroad.[127] Many of the importing countries operate under authoritarian governments, which use surveillance technology for political suppression.[128] But it is not just authoritarian states that are importing Chinese tech or conducting ‘smart city’ exchanges. In 2019, for example, the city of Darwin adopted the ‘smart city’ platform and Australian officials travelled to China to be trained on its use.[129]

A further risk is that through the technology infrastructure they are exporting, Chinese technology companies may be compelled by the Chinese government to allow access to their data via backdoors into their systems, and to feed that data back to Chinese central authorities.[130]

While the pandemic and subsequent economic downturn have slowed the progress on the physical infrastructure project components of the BRI, China has continued to emphasise the Health Silk Road and Digital Silk Road components of the Initiative.[131] Recognising the accelerating migration of consumption, retail, services, and social activities in the era of physical distancing, Chinese companies will look for opportunities in the BRI, including those in medtech (medical technologies ranging from capital equipment to biomaterials and implant innovations), as well as in AI surveillance for virus tracking.

These technospheres also directly provide China with that most valuable commodity — 'the new oil' — data.

In the countries participating in the digital BRI, China is expanding more than its market share through exports of its technology, tech infrastructure, and norms. It is also broadening and deepening its ‘technospheres’ — geographic areas where China has political, economic, and data- and intelligence-gathering advantages due to its export of technology and information management control mechanisms within the BRI.[132] These technospheres also directly provide China with that most valuable commodity — 'the new oil' — data. Through Digital Silk Road agreements backed by the Chinese government, Chinese companies secure legal rights to data collected via Chinese tech embedded in infrastructure projects.[133]

IMPLICATIONS FOR DEMOCRACIES

The expansion and entrenchment of the digital authoritarianism model through the pandemic has significant implications for the health of democracy worldwide. Technology-receiving countries, especially those persuaded of the efficacy of surveillance security models, look to digital technology leaders such as China for inspiration, and for systems to adopt in their own countries. This may predispose them to support China in its efforts to secure global influence in international bodies that will shape the future norms of cyberspace, AI, and digital technologies.

The expansion and entrenchment of the digital authoritarianism model through the pandemic has significant implications for the health of democracy worldwide.

For more established democracies, the creeping acceptance of digital authoritarianism risks a lapse in the regulation of technology and checks on the collection and use of personal data, and the acceptance of mass surveillance. For example, the United States, the origin of immense digital innovation, has tolerated and so far failed to regulate 'surveillance capitalism' — the market-driven sale of personal data.[134] This failure to regulate has allowed major technology companies to amass huge amounts of information that can be deployed to condition and modify individual behaviour for profit. Democracies' permissiveness has allowed the digital communications sector to develop in a way that has exacerbated polarisation, seeded disinformation, and compromised the value of objective facts.[135]

Mass surveillance and the use of facial recognition technology has increasingly become a feature of democratic societies as well — often with little public consultation or awareness. Biometric data is used for identification purposes, CCTV cameras are in place in the public square, and drones are deployed for surveillance. During the pandemic, these technologies have also been used to monitor social distancing, and to detect breaches of health safety directives.[136]

The COVID-19 crisis — in which democracies have come under their first extended states of emergency since the wartime era — illustrates how democratic societies can tolerate the expansion of executive power and become habituated to restrictions on liberties and increased monitoring — particularly if they are managed via inconspicuous or convenient digital technology. Many democracies have accepted new infringements on privacy, bypassing the usual legislative processes of scrutiny and consideration in the interests of pandemic mitigation.[137]

Cheng Hui, head of JDX R&D Center, JD.com, speaks during the session Unleashing the Drone Economy *at the Economic World Forum on Afric 2019. Image: Greg Beadle/World Economic Forum.*

Cyber surveillance and data collection are being conducted to aid public health measures before adequate safeguards have been proven or guaranteed. It will be left to the vigilance of citizens, legislatures, and courts to reassert rights once the emergency is over. In an era of 'global democratic recession', even established democracies cannot be sanguine about maintaining civil liberties and constitutional safeguards.[138]

CONCLUSION

China’s pandemic response, underwritten by an expansion of its digital authoritarianism, is a critical part of its efforts to boost its footing on the world stage.[139] With US global leadership on the retreat, but pressure on the CCP mounting, China has found an opening: highlighting the country’s success in supressing the pandemic and encouraging other countries to deploy Beijing’s pandemic playbook.[140] While President Trump abdicates global leadership and the United States flails in its pandemic response, China has not wavered on its strategic ambitions, nor on the future technology through which it aspires to transform the strategic stage.

The COVID-19 pandemic has already shaped the future.[141] Among its many legacies are the normalisation of technological surveillance, the notion of the surveillance state, and China's opportunistic advancement of its technology agenda. The onus is on democracies to do more to counter the harmful aspects of China’s global technology agenda, and to find ways to harness technology, including AI, for the global public good while preserving hard-won democratic rights and liberties.

NOTES

[1] Human Rights Watch, *Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights*, 2 April 2020, https://www. hrw. org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight.

[2] China's *People* magazine.

[3] Lily Kuo, "Coronavirus: Wuhan Doctor Speaks Out Against Authorities", *The Guardian,* 11 March 2020, https://www.theguardian.com/world/2020/mar/11/coronavirus-wuhan-doctor-ai-fen-speaks-out-against-authorities.

[4] "Dr Ai Fen, the Wuhan Whistle", translated in *Science Integrity Digest,* 11 March 2020, https://scienceintegritydigest. com/2020/03/11/dr-ai-fen-the-wuhan-whistle/.

[5] "China's Online Censors Tighten Grip after Brief Coronavirus Respite", Reuters, 11 February 2020, https://www.reuters.com/article/us-china-health-censorship/chinas-online-censors-tighten-grip-after-brief-coronavirus-respite-idUSKBN2051BP.

[6] Helen Davidson, "Chinese Inquiry Exonerates Coronavirus Whistleblower Doctor", *The Guardian,* 20 March 2020, https://www.theguardian.com/world/2020/mar/20/chinese-inquiry-exonerates-coronavirus-whistleblower-doctor-li-wenliang.

[7] "China Releases Investigation Report on Issues Concerning Dr Li Wenliang", *China.org.cn,* 20 March 2020 http://www. china. org. cn/china/2020-03/20/content_75836863. htm.

[8] Gerry Shih, "Doctor's Death from Coronavirus Sparks a Digital Uprising, Rattling China's Leaders", *Washington Post*, 8 February 2020, https://www.washingtonpost.com/world/asia_pacific/doctors-death-from-coronavirus-sparks-a-digital-uprising-rattling-chinas-leaders/2020/02/07/a4cb3492-4998-11ea-8a1f-de1597be6cbc_story.html; Verna Yu, "'Hero Who Told the Truth': Chinese Rage over Coronavirus Death of Whistleblower Doctor", *The Guardian,* 7 February 2020, https://www.theguardian.com/global-development/2020/feb/07/coronavirus-chinese-rage-death-whistleblower-doctor-li-wenliang.

[9] Paul Mozur, "Coronavirus Outrage Spurs China's Internet Police to Action", *The New York Times,* 16 March 2020, https://www.nytimes.com/2020/03/16/business/china-coronavirus-internet-police.html.

[10] Lily Kuo, "'Sacrificed': Anger in China over Death of Wuhan Doctor from Coronavirus", *The Guardian,* 3 June 2020, https://www.theguardian.com/world/2020/jun/03/sacrificed-anger-in-china-over-death-of-wuhan-doctor-from-coronavirus.

[11] "Whistleblowers Silenced by China Could Have Stopped Global Coronavirus Spread", 60 Minutes, 29 March 2020, https://www. youtube. com/watch?v=pEQcvcyzQGE.

[12] "Chinese Doctor Says She is Safe and Well amid Concern She Was Detained", Radio Free Asia, 14 April 2020, https://www.rfa.org/english/news/china/wuhan-doctor-04142020114914.html.

[13] Ryan Broderick, "Chinese WeChat Users Are Sharing a Censored Post about COVID-19 by Filling it with Emojis and Writing it in Other Languages", *Buzzfeed News,* 11 March 2020, https://www. buzzfeednews. com/article/ryanhatesthis/coronavirus-covid-chinese-wechat-censored-post-emojis.

[14] "Internal Chinese Report Warns Beijing Faces Tiananmen-like Global Backlash over Virus", Reuters, 4 May 2020, https://www. reuters. com/article/us-health-coronavirus-china-sentiment-ex/exclusive-internal-chinese-report-warns-beijing-faces-tiananmen-like-global-backlash-over-virus-idUSKBN22G19C.

[15] Shengjie Lai, et al, "Effect of Non-pharmaceutical Interventions for Containing the COVID-19 Outbreak in China", *MedRxiv*, 3 March 2020, https://doi.org/10.1101/2020.03.03.20029843.

[16] Sophia Beach, "Minitrue: Do Not Transmit Video and Images of Law Enforcement Actions around COVID-19 Prevention", *China Digital Times,* 13 March 2020, https://chinadigitaltimes. net/2020/03/minitrue-do-not-transmit-video-and-images-of-law-enforcements-actions-around-covid-19-prevention/.

[17] See, for example, "Coronavirus-era Repression, Propaganda, Censorship, Surveillance and More", China Media Bulletin 142, Freedom House, March 2020, https://freedomhouse.org/report/china-media-bulletin/2020/china-media-bulletin-coronavirus-era-repression-propaganda.

[18] Laura Rosenberger, "China's Coronavirus Information Offensive", *Foreign Affairs,* 22 April 2020, https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive.

[19] "Grid-based Communication Workers Power Up China's Grassroots Coronavirus Fight", *Xinhua,* 1 March 2020, http://www. xinhuanet.

com/english/2020-03/01/c_138832911. htm. *Wanggehua guanli*, or grid management, is a netted management system where a local territory is divided into a number of segments, with each segment being monitored by a designated person who submits the information to a designated government authority on a regular basis. See Yongshun Cai, "Grid Management and Social Control in China", *The Asia Dialogue,* 27 April 2018, https://theasiadialogue.com/2018/04/27/grid-management-and-social-control-in-china/.

[20] Jeff John Roberts, "The Splinternet is Growing", *Fortune,* 29 May 2019, https://fortune. com/2019/05/29/splinternet-online-censorship/.

[21] Justin Sherman, "The Long View of Digital Authoritarianism", *New America,* 20 June 2019 https://www.newamerica.org/weekly/long-view-digital-authoritarianism/.

[22] Adrian Shahbaz and Allie Funk, *Freedom on the Net 2019: The Crisis of Social Media*, Freedom House, 2019, https://freedomhouse. org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download. pdf.

[23] Samantha Hoffman, *Engineering Global Consent: The Chinese Communist Party's Data-driven Power Expansion*, ASPI Policy Brief Report No 21/2019, Australian Strategic Policy Institute International Cyber Policy Centre, 14 October 2019, https://www. aspi. org. au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[24] Ibid.

[25] Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House, 2018, https://freedomhouse. org/report/freedom-net/2018/rise-digital-authoritarianism.

[26] Ibid.

[27] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: the Russian and Chinese Models", *Brookings Institution,* August 2019, https://www. brookings. edu/research/exporting-digital-authoritarianism/.

[28] See Richard McGregor, *Xi Jinping: The Backlash,* (Sydney: Penguin, 2019), for a discussion of President Xi's authoritarian control of China.

[29] Ross Andersen, "The Panopticon is Already Here", *The Atlantic,* September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

[30] Interview by author with Samantha Hoffman, analyst at Australian Strategic Policy Institute, 4 September 2020.

[31] Katherine Manstead, "Strong Yet Brittle: The Risks of Digital Authoritarianism", *Alliance for Securing Democracy*, 28 May 2020, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/05/Strong-Yet-Brittle-The-Risks-of-Digital-Authoritarianism.pdf.

[32] John Lee, "The Rise of China's Tech Sector: The Making of an Internet Empire", The Interpreter, 4 May 2017, https://www. lowyinstitute. org/the-interpreter/rise-china-s-tech-sector-making-internet-empire.

[33] Louise Lucas, "Why the Wheels Fell off China's Tech Boom", *Financial Times,* 21 July 2019, https://www. ft. com/content/24fd72be-92bb-11e9-aea1-2b1d33ac3271.

[34] Danielle Cave, et al, *Mapping China's Technology Giants*, Report No 15/2019, Australian Strategic Policy Institute International Cyber Policy Centre, 18 April 2019, https://www. aspi. org. au/report/mapping-chinas-tech-giants/.

[35] See Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House, https://freedomhouse. org/report/freedom-net/2018/rise-digital-authoritarianism, in particular the section on "Chinese Companies under the Spotlight"; William Turton, "Hidden Back Door Embedded in Chinese Tax Software, Firm Says", *Bloomberg*, 25 June 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.

[36] Samantha Hoffman, "China's Tech-Enhanced Authoritarianism", written testimony before the House Permanent Select Committee on Intelligence Hearing on "China's Digital Authoritarianism: Surveillance, Influence, and Political Control", 1, 16 May 2019, https://docs. house. gov/meetings/IG/IG00/20190516/109462/HHRG-116-IG00-Wstate-HoffmanS-20190516. pdf.

[37] Louise Lucas, "China Government Assigns Officials to Companies Including Alibaba", *Financial Times,* 23 September 2019, https://www. ft. com/content/055a1864-ddd3-11e9-b112-9624ec9edc59.

[38] Tom Simonite, "Behind the Rise of China's Facial Recognition Giants", *Wired,* 3 September 2019, https://www. wired. com/story/behind-rise-chinas-facial-recognition-giants/.

[39] Elizabeth Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown", *The Guardian,* 29 June 2018, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

[40] Data sent over computer networks, such as the internet, is divided into smaller 'packets' that are then reconfigured by the computer that is receiving them. Deep packet inspection is able to check the content of the packets, know where it came from and where it is going, and can block or redirect its final destination. Deep packet inspection is an advanced way to examine and manage network traffic, usually part of a firewall. See Duncan Geere, "How Deep Packet Inspection Works", *Wired,* 27 April 2012, https://www.wired.co.uk/article/how-deep-packet-inspection-works . See also, Young Xu, "Deconstructing the Great Firewall of China", *Thousand Eyes,* 8 March 2016, https://blog.thousandeyes.com/deconstructing-great-firewall-china/.

[41] Stephen McDonell, "China Social Media: WeChat and the Surveillance State" BBC News, 7 June 2019, https://www. bbc. com/news/blogs-china-blog-48552907.

[42] Lotus Ruan, et al, "Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media", *The Citizen Lab,* 3 March 2020, https://citizenlab. ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

[43] Jeffrey Knockel, et al, "We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus", Research Report #127, *The Citizen Lab,* 7 May 2020, https://citizenlab. ca/2020/05/we-chat-they-watch/.

[44] Paul Mozur, "Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras", *The New York Times,* 8 July 2018, https://www. nytimes. com/2018/07/08/business/china-surveillance-technology. html.

[45] Interview by author with Samantha Hoffman, analyst at Australian Strategic Policy Institute, 4 September 2020.

[46] Ibid.

[47] Josh Rudolph, "Sharper Eyes: Surveilling the Surveillers (Part 1)", *China Digital Times,* 9 September 2019, https://chinadigitaltimes. net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1/.

[48] Simon Denyer, "China's Watchful Eye", *Washington Post,* 7 January 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.

[49] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using AI to Profile a Minority", *The New York Times,* 14 April 2019, https://www. nytimes. com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling. html.

[50] "State Council Notice Concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020)", State Council, 14 June 2014, edited translation: https://chinacopyrightandmedia.wordpress. com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/.

[51] Ibid.

[52] Chris Fei Shen, "Social Credit System in China", City University of Hong Kong, March 2019, https://www. researchgate.net/publication/331733377_Social_Credit_System_in_China.

[53] "Understanding China's Social Credit System", *Truvium China,* 27 August, 2019, http://socialcredit.triviumchina.com/wp-content/uploads/2019/09/Understanding-Chinas-Social-Credit-System-Trivium-China-20190923.pdf.

[54] Nicole Kobie, "The Complicated Truth about China's Social Credit System", *Wired,* 7 June 2019, https://www. wired. co. uk/article/china-social-credit-system-explained.

[55] Ibid.

[56] Yin Yijun, "Chinese App Gives Blacklisted People 'Dishonest' Caller ID", *Sixth Tone,* 30 August 2017, https://www. sixthtone.com/news/1000762/chinese-app-gives-blacklisted-people-dishonest-caller-id.

[57] Nicole Kobie, "The Complicated Truth about China's Social Credit System", https://www. wired. co. uk/article/china-social-credit-system-explained.

[58] Christina Zhou and Bang Xiao, "China's Social Credit System is Pegged to be Fully Operational by 2020 — But What Will it Look Like?", ABC News, 2 January 2020, https://www. abc. net. au/news/2020-01-02/china-social-credit-system-operational-by-2020/11764740.

[59] Interview by author with Samantha Hoffman, analyst at Australian Strategic Policy Institute, 4 September 2020.

[60] Renee Xia and Frances Eve, "'A Healthy Society Should Not Have Just One Voice'— China Must End Crackdown on Online Speech in Response to COVID-19", *Chinese Human Rights Defenders,* 1 April 2020, https://www.nchrd. org/2020/04/a-healthy-society-should-not-have-just-one-voice-china-must-end-crackdown-on-online-speech-in-response-to-covid-19/.

[61] Verna Yu and Emma Graham-Harrison, "'This May Be the Last Piece I Write': Prominent Xi Critic has Internet Cut after House Arrest", *The Guardian,* 16 February 2020, https://www. theguardian. com/world/2020/feb/15/xi-critic-professor-this-may-be-last-piece-i-write-words-ring-true.

[62] Xu Zhangrun (translated by Geremie R Barme), “Viral Alarm: When Fury Overcomes Fear”, *The China File,* 10 February 2020, https://www. chinafile. com/reporting-opinion/viewpoint/viral-alarm-when-fury-overcomes-fear.

[63] Wong Lok-to and Gao Feng, “Police Arrest Professor Who Linked Virus to Chinese Communist Party”, Radio Free Asia, 5 April 2020, https://www.rfa.org/english/news/china/professor-05042020132931.html.

[64] Gao Feng, “China Holds Three Activists Linked to Censored Articles about Coronavirus”, Radio Free Asia, 28 April 2020, https://www. rfa. org/english/news/china/holds-04282020103115. html

[65] Renee Xia and Frances Eve, “’A Healthy Society Should Not Have Just One Voice’ — China Must End Crackdown on Online Speech in Response to COVID-19”, https://www. nchrd. org/2020/04/a-healthy-society-should-not-have-just-one-voice-china-must-end-crackdown-on-online-speech-in-response-to-covid-19/.

[66] Lotus Ruan, et al, “Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media”, Research Report #126, *The Citizen Lab*, 3 March 2020, https://citizenlab. ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

[67] Li Yuan, “Widespread Outcry in China over Death of Coronavirus Doctor”, *The New York Times,* 7 February 2020, https://www. nytimes. com/2020/02/07/business/china-coronavirus-doctor-death. html.

[68] Javier C Hernandez, “China Spins Coronavirus Crisis, Hailing Itself as a Global Leader”, *The New York Times,* 28 February 2020, https://www. nytimes. com/2020/02/28/world/asia/china-coronavirus-response-propaganda. html.

[69] “New Disinformation Tactics, Coronavirus Censorships, Activist Arrests”, China Media Bulletin 144, Freedom House, May 2020, https://freedomhouse. org/report/china-media-bulletin/2020/new-disinformation-tactics-coronavirus-censorship-activist-arrests. See also Natasha Kassam, *Lowy Institute Poll 2020*, Lowy Institute, 24 June 2020, https://poll. lowyinstitute. org/report/.

[70] “Grid-based Communication Workers Power Up China’s Grassroots Coronavirus Fight”, *Xinhua,* 1 March 2020, http://www. xinhuanet. com/english/2020-03/01/c_138832911. htm. See also, Liza Lin, “China Marshals its Surveillance Powers against Coronavirus”, *The Wall Street Journal,* 4 February 2020, https://www. wsj. com/articles/china-

marshals-the-power-of-its-surveillance-state-in-fight-against-coronavirus-11580831633.

[71] Yingzhi Yang and Julie Zhu, "Coronavirus Brings China's Surveillance State Out of the Shadows", Reuters, 7 February 2020, https://www. reuters. com/article/us-china-health-surveillance/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO.

[72] Charlie Campbell, "'The Entire System is Designed to Supress Us.' What the Chinese Surveillance State Means for the Rest of the World", *Time*, 21 November 2019, https://time.com/5735411/china-surveillance-privacy-issues/. See also, Hilary Osborne and Sam Cutler, "Chinese Border Guards Put Secret Surveillance App on Tourists' Phones", *The Guardian,* 3 July 2019, https://www. theguardian. com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones.

[73] Nectar Gan, "China is Installing Surveillance Cameras Outside People's Front Doors … and Sometimes Inside Their Homes", CNN Business, 28 April 2020, https://edition. cnn. com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index. html.

[74] Lily Kuo, "'The New Normal': China's Excessive Coronavirus Public Monitoring Could be Here to Stay", *The Guardian,* 9 March 2020, https://www. theguardian. com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

[75] Shawn Yuan, "How China is Using AI and Big Data to Fight the Coronavirus", Al Jazeera, 1 March 2020, https://www. aljazeera. com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951. html.

[76] Shona Ghosh, "Police in China, Dubai, and Italy are Using these Surveillance Helmets to Scan People for COVID-19 Fever as they Walk Past and it May be our Future Normal", *Business Insider,* 17 May 2020, https://www. businessinsider. com. au/coronavirus-italy-holland-china-temperature-scanning-helmets-2020-5?r=US&IR=T.

[77] Ali Dukakis, "China Rolls out Software Surveillance for the COVID-19 Pandemic, Alarming Human Rights Advocates", ABC News, 14 April 2020, https://abcnews. go. com/International/china-rolls-software-surveillance-covid-19-pandemic-alarming/story?id=70131355.

[78] See further discussion in the "Technology Exports and the Belt and Road Initiative" section below.

[79] Patrick Howell O'Neill, et al, "Covid Tracing Tracker: A Flood of Coronavirus Apps are Tracking Us. Now It's Time to Keep Track of Them", *MIT Technology Review,* 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-

mittr-covid-tracing-tracker/. See MIT Technology Review's Covid Tracing Tracker, https://public.flourish.studio/visualisation/2241702/.

[80] Yuan Yang and Nian Liu, "China Survey Shows High Concern over Facial Recognition Abuse", *Financial Times,* 5 December 2019, https://www. ft. com/content/7c32c7a8-172e-11ea-9ee4-11f260415385.

[81] Paul Mozur, "China, Desperate to Stop Coronavirus, Turns Neighbor against Neighbor", *The New York Times,* 3 February 2020, https://www. nytimes. com/2020/02/03/business/china-coronavirus-wuhan-surveillance. html.

[82] Yuan Yang, et al, "China, Coronavirus and Surveillance: The Messy Reality of Personal Data", *Financial Times,* 2 April 2020, https://www. ft. com/content/760142e6-740e-11ea-95fe-fcd274e920ca.

[83] Arjun Kharpal, "Coronavirus Could be a 'Catalyst' for China to Boost its Mass Surveillance Machine, Experts Say", CNBC, 24 February 2020, https://www. cnbc. com/2020/02/25/coronavirus-china-to-boost-mass-surveillance-machine-experts-say. html.

[84]Lily Kuo, "'The New Normal': China's Excessive Coronavirus Public Monitoring Could be Here to Stay", https://www. theguardian. com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

[85] Raymond Zhong, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears", *The New York Times,* 26 May 2020, https://www. nytimes. com/2020/05/26/technology/china-coronavirus-surveillance. html.

[86] Ibid.

[87] Christina Gigler and Kai Kang, "China's Social Credit System in the Light of COVID-19", *Roedl and Partner Insights,* 17 April 2020, https://www.roedl.com/insights/covid-19/coronavirus-china-social-credit-system.

[88] "Coronavirus: Chinese Authorities Leverage Social Credit in the Fight Against COVID-19", *Trivium Social Credit,* 21 February 2020, http://socialcredit. triviumchina. com/2020/02/coronavirus-chinese-authorities-leverage-social-credit-in-the-fight-against-covid-19/.

[89] Raymond Zhong, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears", https://www. nytimes. com/2020/05/26/technology/china-coronavirus-surveillance. html.

[90] Lu Qi, "Representative Cheng Jing: Establishing a 'Skynet' for Smart Surveillance of Major Epidemics", *Science.net.cn,* 20 May 2020, http://news. sciencenet. cn/htmlnews/2020/5/440102. shtm.

[91] Ibid.

[92] Masha Borak, “Chinese Scientist Want a New Skynet-like System Just for Tracking Viruses”, *South China Morning Post,* 22 May 2020, https://www.scmp. com/abacus/tech/article/3085543/chinese-scientist-wants-new-skynet-system-just-tracking-viruses.

[93] Ben Westcott and Steven Jiang, “China is Embracing a New Brand of Foreign Policy. Here’s What Wolf Warrior Diplomacy Means”, CNN, 29 May 2020, https://edition.cnn.com/2020/05/28/asia/china-wolf-warrior-diplomacy-intl-hnk/index.html.

[94] Laura Silver, Kat Devlin and Christine Huang, “Unfavorable Views of China Reach Historic Highs in Many Countries”, Pew Research Center, *Global Attitudes and Trends*, 6 October 2020, https://www.pewresearch.org/global/2020/10/06/unfavorable-views-of-china-reach-historic-highs-in-many-countries/.

[95] Laura Silver, Kat Devlin and Christine Huang, “2. Attitudes Toward China”, Pew Research Center, *Global Attitudes and Trends*, 5 December 2019, https://www.pewresearch.org/global/2019/12/05/attitudes-toward-china-2019/.

[96] Natasha Kassam, et al, “How Is The Coronavirus Outbreak Affecting China’s Relations with Its Asian Neighbors?” *China File*, 26 April 2020, https://www.chinafile.com/conversation/how-coronavirus-outbreak-affecting-chinas-relations-its-asian-neighbors.

[97] Nadège Rolland, “China’s Pandemic Power Play”, *Journal of Democracy,* Vol 31, Issue 3, July 2020, https://www. journalofdemocracy. org/articles/chinas-pandemic-power-play-2/.

[98] Li Qingqing and Yan Yunming, “US Seeks Selfish Gains as China Goes All Out to Control Coronavirus Spread”, *Global Times,* 2 April 2020, http://www. globaltimes. cn/content/1178494. shtml.

[99] Jordan Hayne, “Australia ‘Hurt the Feelings’ of China With Calls for Coronavirus Investigation, Senior Diplomat Says” ABC News, 26 August 2020, https://www.abc.net.au/news/2020-08-26/senior-chinese-diplomat-addresses-australia-coronavirus-tensions/12596602.

[100] Zhao Lijian Twitter feed, 13 March 2020, https://twitter.com/zlj517/status/1238111898828066823.

[101] Kate Conger, “Twitter Removes Chinese Disinformation Campaign”, *The New York Times,* 11 June 2020, https://www.nytimes.com/2020/06/11/technology/twitter-chinese-misinformation.html.

[102] Mark Scott, et al, “European Commission Accuses China of Peddling Disinformation”, *Politico*, 10 June 2020,

https://www.politico.eu/article/european-commission-disinformation-china-coronavirus/.

[103] Rick Sarre, "Melbourne is Using Pop-Up Police Spy Stations to Find People Breaking COVID Rules – What Does the Law Say?", *The Conversation*, 11 September 2020, https://theconversation.com/melbourne-is-using-pop-up-police-spy-stations-to-find-people-breaking-covid-rules-what-does-the-law-say-145684.

[104] Arjun Kharpal, "Coronavirus Could be a 'Catalyst' for China to Boost Its Mass Surveillance Machine, Experts Say". https://www. cnbc. com/2020/02/25/coronavirus-china-to-boost-mass-surveillance-machine-experts-say. html.

[105] Patrick Howell O'Neill, et al, "Covid Tracing Tracker: A Flood of Coronavirus Apps are Tracking Us. Now It's Time to Keep Track of Them", *MIT Technology Review,* 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. See MIT Technology Review's Covid Tracing Tracker, https://public.flourish.studio/visualisation/2241702/.

[106] Alfred Ng, "COVID-19 Could Set a New Norm for Surveillance and Privacy", *CNET,* 11 May 2020, https://www. cnet. com/health/covid-19-could-set-a-new-norm-for-surveillance-and-privacy/.

[107] Human Rights Watch, *Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights*", 2 April 2020, https://www. hrw. org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight.

[108] Jake Goldenfein, et al, "Privacy Versus Health is a False Trade Off", *Jacobin Magazine,* 17 April 2020, https://jacobinmag. com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology.

[109] David Pilling, "WHO Chief Splits Opinion with Praise for China's Virus Fight", *Financial Times,* 8 February, https://w9www. ft. com/content/57c6a1d6-49a7-11ea-aeb3-955839e06441.

[110] Xifeng Wu, et al, "6 Lessons from China's Zhejiang Province and Hangzhou on How Countries Can Prevent and Rebound from an Epidemic Like COVID-19", *World Economic Forum COVID Action Platform,* 12 March 2020, https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-hangzhou-zhejiang-government-response/.

[111] Sarah Cook, "China's Cyber Superpower Strategy: Implementation, Internet Freedom Implications and US Responses", Written Testimony for the House Committee on Oversight and Government Reform, Subcommittee on Information Technology, 26 September 2018, https://republicans-oversight. house. gov/wp-

content/uploads/2018/09/Cook-FreedomHouse-Statement-China-9-26.pdf.

[112] "Made in China 2025 Plan Issued", State Council, The People's Republic of China, Press Release, 19 May 2015, http://english. www. gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

[113] James McBride and Andrew Chatzky, "Is 'Made in 2025' a Threat to Global Trade?" Council on Foreign Relations, 13 May 2019, https://www. cfr.org/backgrounder/made-china-2025-threat-global-trade.

[114] Anna Gross, et al, "Chinese Tech Groups Shaping UN Facial Recognition Standards", *Financial Times,* 2 December 2019, https://www. ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67.

[115] Arjun Kharpal, "Power is 'Up for Grabs': Behind China's Plan to Shape the Future of Next-generation Tech", CNBC, 26 April 2020, https://www.cnbc. com/2020/04/27/china-standards-2035-explained. html.

[116] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: the Russian and Chinese Models", *Brookings Institution,* August 2019, https://www. brookings. edu/research/exporting-digital-authoritarianism/.

[117] See section on "Big Tech" in "China's Digital Authoritarian Model" above.

[118] Christopher Balding and Donald C Clarke, "Who Owns Huawei?" Social Science Research Network, 17 April 2019, https://papers. ssrn.com/abstract=3372669.

[119] Edward Zhang, "How Will the Coronavirus Impact Xi's 'Made in China 2025' Plan?", *Medium*, 12 May 2020, https://medium. com/wonk-bridge/how-will-the-coronavirus-impact-xis-made-in-china-2025-plan-db55c31c6f4a.

[120] Jaron Lanier and Glen Weyl, "AI is an Ideology Not a Technology", *Wired,* 15 March 2020, https://www. wired. com/story/opinion-ai-is-an-ideology-not-a-technology/.

[121] Jason Cohen, "The World Relies on China's Surveillance Technology", *PC Magazine,* 13 December 2019, https://au. pcmag. com/news/64899/the-world-relies-on-chinas-surveillance-technology.

[122] Shona Ghosh, "Police in China, Dubai, and Italy are Using these Surveillance Helmets to Scan People for COVID-19 Fever as they Walk Past and It May be our Future Normal", *Business Insider Australia*, 17 May 2020, https://www. businessinsider. com. au/coronavirus-italy-holland-china-temperature-scanning-helmets-2020-5?r=US&IR=T.

[123] Thomas S Eder, et al, “Networking the ‘Belt and Road’ — The Future is Digital”, Analysis, *MERICS — Mercator Institute for China Studies*, 28 August 2019, https://merics. org/en/analysis/networking-belt-and-road-future-digital.

[124] Sheena Chestnut Greitens, “Dealing with Demand for China’s Global Surveillance Exports”, *Brookings Institution Global China Report,* April 2020, https://www. brookings. edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/.

[125] Ibid. Greitens appears to have drawn on the data gathered for ASPI’s Mapping China’s Technology Giants project available, https://chinatechmap.aspi.org.au.

[126] Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House, 2018, https://freedomhouse. org/report/freedom-net/2018/rise-digital-authoritarianism. See also, Joe Parkinson, et al, “Huawei Technicians Help African Governments Spy on Political Opponents”, *Wall Street Journal,* 15 August 2019, https://www. wsj. com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[127] Tom Simonite, “Behind the Rise of China’s Facial Recognition Giants”, *Wired,* 3 September 2019, https://www. wired. com/story/behind-rise-chinas-facial-recognition-giants/.

[128] Steven Feldstein, “The Global Expansion of AI Surveillance”, Paper — Carnegie Endowment for International Peace, 17 September 2019, https://carnegieendowment. org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847,%20p. 13.

[129] “Council to Return to Shenzhen for Final Assessments as Smart City Project Comes to an End”, *The West Australian*, 14 April 2019, https://thewest.com.au/news/nt/council-to-return-to-shenzhen-for-final-assessments-as-smart-city-project-comes-to-an-end-ng-06de2544dd5238fb4edeeb9d5e88139c.

[130] Shahbaz, *Freedom on the Net 2018*; Turton, “Hidden Back Door”.

[131] Iain Marlow, et al, “China’s Belt and Road Plan is Getting Lashed by Coronavirus”, Bloomberg, 5 March 2020, https://www.bloomberg.com/news/articles/2020-03-04/china-s-grand-belt-and-road-plan-is-being-lashed-by-coronavirus. See also, Xianbai Ji, “Will COVID-19 be a Blessing in Disguise for the Belt and Road?” *The Diplomat,* 2 May 2020, https://thediplomat. com/2020/05/will-covid-19-be-a-blessing-in-disguise-for-the-belt-and-road/.

[132] Valentin Weber, *The Worldwide Web of Chinese and Russian Information Controls*, Open Technology Fund, 2018, https://public. opentech.

fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf.

[133] Lynsey Chutel, "China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database", *Quartz Africa,* 25 May 2018, https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/.

[134] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: Public Affairs, 2019).

[135] Seva Gunitsky, "The Great Online Convergence: Digital Authoritarianism Comes to Democracies", *War on the Rocks,* 19 February 2020, https://warontherocks. com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/.

[136] Cameron Houston, "'No Justification': Anger over Mobile Public Surveillance Units at Public Parks", *The Age*, 6 September 2020, https://www.theage.com.au/national/victoria/no-justification-anger-over-mobile-surveillance-units-at-public-parks-20200906-p55svg.html.

[137] Carrie Cordero and Richard Fontaine, "Health Surveillance is Here to Stay", *Wall Street Journal,* 27 March 2020, https://www.wsj.com/articles/health-surveillance-is-here-to-stay-11585339451.

[138] Larry Diamond, "Facing Up to the Democratic Recession", *Journal of Democracy,* Vol 26, Issue 1, January 2015, https://www. journalofdemocracy. org/articles/facing-up-to-the-democratic-recession/.

[139] Steven Lee Myers and Alissa J Rubin, "Its Coronavirus Cases Dwindling, China Turns Focus Outward", *The New York Times*, 18 March 2020, https://www. nytimes. com/2020/03/18/world/asia/coronavirus-china-aid. html.

[140] Nadège Rolland, "China's Pandemic Power Play", *Journal of Democracy,* Vol 31, Issue 3, July 2020, https://www. journalofdemocracy. org/articles/chinas-pandemic-power-play-2/.

[141] *The World After COVID-19*, Lowy Institute, https://interactives.lowyinstitute.org/features/covid19/.

ABOUT THE AUTHOR

Lydia Khalil

Lydia Khalil is a Research Fellow in the West Asia Program at the Lowy Institute.

She has a broad range of policy, academic and private sector experience, and has spent her career focusing on the intersection between governance and security — whether it be understanding the rationales behind terrorism and counterinsurgency, how to create governance systems that lead to functioning societies, effective policing strategies or the security and policy effects of new technology. She is currently a director of Arcana Partners, a strategic consultancy firm.

Lydia's professional background in politics, international relations and security has focused on US national security policy, Middle East politics and intelligence. She was international affairs fellow at the Council on Foreign Relations in New York where she analysed political and security trends in the Middle East. She also served as a political advisor for the US Department of Defense in Iraq, where she worked closely with Iraqi officials on political negotiations and constitutional drafting. In Australia, Lydia held fellowships with the Australian Strategic Policy Institute and Macquarie University, specialising in intelligence, national security and cyber security.

Lydia also has extensive national security and law enforcement experience. She was most recently a senior policy advisor to the Boston Police Department, working on countering violent extremism, intelligence and counterterrorism, and community policing strategies. She has also worked as a senior counterterrorism and intelligence analyst for the New York Police Department.

Lydia is a frequent media commentator and conference speaker and has published widely on her areas of expertise. She holds a BA in International Relations from Boston College and a Masters in International Security from Georgetown University.

LOWY INSTITUTE

31 Bligh Street
Sydney NSW 2000

Tel. +61 2 8238 9000
Fax +61 2 8238 9005

lowyinstitute.org
@LowyInstitute