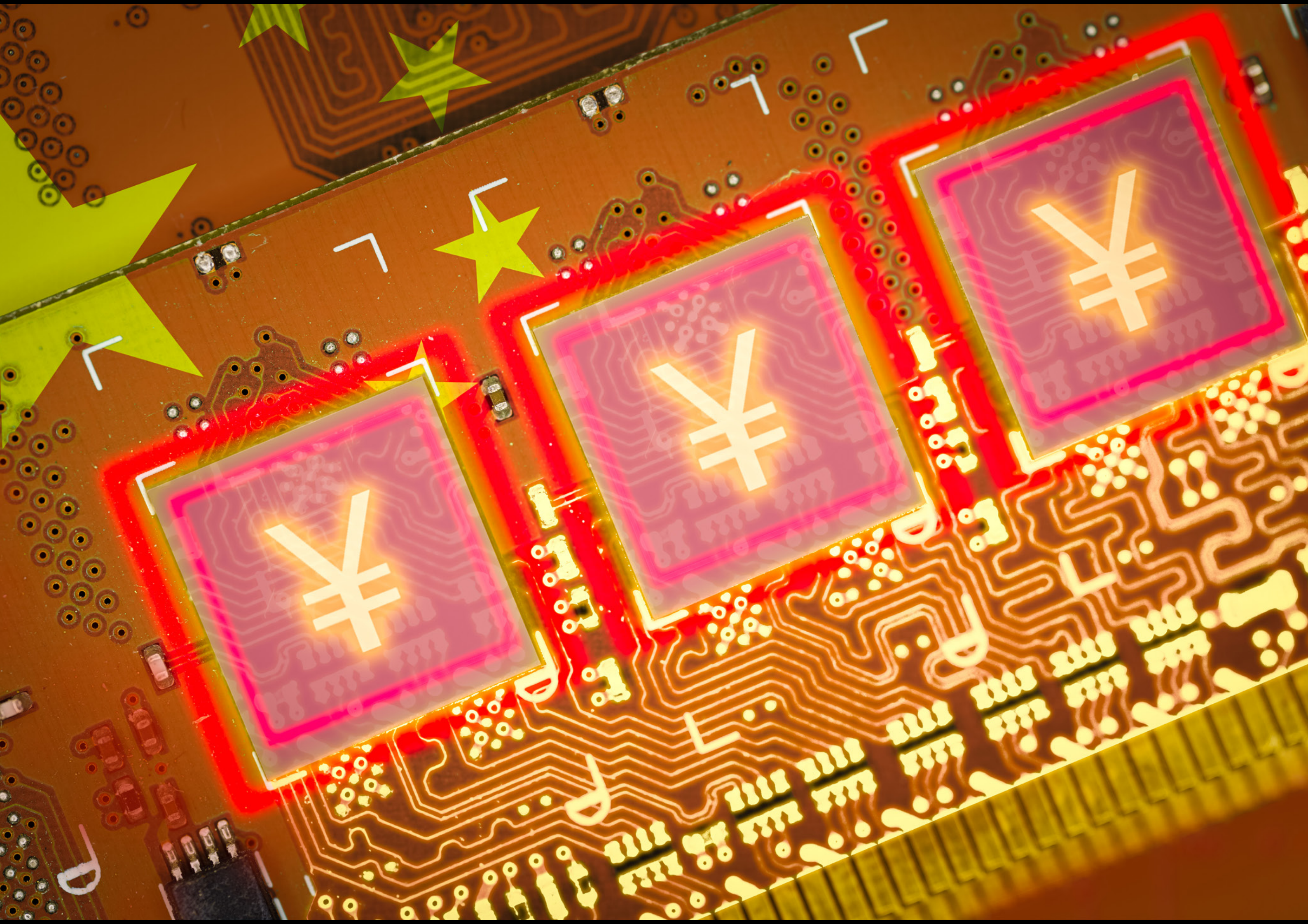
De-risking authoritarian AI

A balanced approach to protecting our digital ecosystems

Simeon Gilding



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief
Report No. 72/2023

About the author

Simeon Gilding is a senior fellow at ASPI and has previously held senior positions across Australia's national security community, including at the Australian Signals Directorate where he was Deputy Director-General responsible for signals intelligence and offensive cyber operations.

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners and custodians of the land upon which this work was prepared, and their continuing connection to land, waters and community. We pay our respects to their cultures, country and elders past, present and emerging.

The author would like to thank all ASPI staff who reviewed the work and supported this project, in particular Danielle Cave, Vahri Fotheringham and Alex Caples. He would also like to thank his external reviewers.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI Cyber, Technology & Security

ASPI's Cyber, Technology & Security (CTS) analysts aim to inform and influence policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS remains a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and Internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity building team that conducts workshops, training programs and large-scale exercises for the public, private and civil society sectors. Current projects are focusing on capacity building in Southeast Asia and the Pacific Islands region, across a wide range of topics. CTS enriches regional debate by collaborating with civil society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on. If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

ASPI

Tel Canberra: +61 2 6270 5100
Tel Washington DC: +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_CTS

First published July 2023.

ISSN 2209-9689 (online).
ISSN 2209-9670 (print).

Cover image: iStockphoto.com/Tanaonte.

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

No specific sponsorship was received to fund production of this report.

De-risking authoritarian AI

A balanced approach to protecting our digital ecosystems

Simeon Gilding

Policy Brief
Report No. 72/2023

Contents

What’s the problem?

Artificial intelligence (AI)–enabled systems make many invisible decisions affecting our health, safety and wealth. They shape what we see, think, feel and choose, they calculate our access to financial benefits as well as our transgressions, and now they can generate complex text, images and code just as a human can, but much faster.

So it’s unsurprising that moves are afoot across democracies to regulate AI’s impact on our individual rights and economic security, notably in the European Union (EU).

But, if we’re wary about AI, we should be even more circumspect about AI-enabled products and services from authoritarian countries that share neither our values nor our interests. And, for the foreseeable future, that means the People’s Republic of China (PRC)—a revisionist authoritarian power demonstrably hostile to democracy and the rules-based international order, which routinely uses AI to strengthen its own political and social stability at the expense of individual human rights. In contrast to other authoritarian countries such as Russia, Iran and North Korea, China is a technology superpower with global capacity and ambitions and is a major exporter of effective, cost-competitive AI-enabled technology into democracies.

In a technology-enabled world, the threats come at us ‘at a pace, scale and reach that is unprecedented’.[1] And, if our reliance on AI is also without precedent, so too is the opportunity—via the magic of the internet and software updates—for remote, large-scale foreign interference, espionage and sabotage through AI-enabled industrial and consumer goods and services inside democracies’ digital ecosystems. AI systems are embedded in our homes, workplaces and essential services. More and more, we trust them to operate as advertised, always be there for us and keep our secrets.

Notwithstanding the honourable intentions of individual vendors of Chinese AI-enabled products and services, they’re subject to direction from PRC security and intelligence agencies, so we in the democracies need to ask ourselves: against the background of growing strategic competition with China, how much risk are we willing to bear?

We should worry about three kinds of Chinese AI-enabled technology:

1. products and services (often physical infrastructure), where PRC ownership exposes democracies to risks of espionage (notably surveillance and data theft) and sabotage (disruption and denial of products and services)
2. AI-enabled technology that facilitates foreign interference (malign covert influence on behalf of a foreign power), the most pervasive example being TikTok
3. ‘Large language model AI’ and other emerging generative AI systems—a future threat that we need to start thinking about now.

While we should address the risks in all three areas, this report focuses more on the first category (and indeed looks at TikTok through the prism of the espionage and sabotage risks that such an app poses).

The underlying dynamic with Chinese AI-enabled products and services is the same as that which prompted concern over Chinese 5G vendors: the PRC Government has the *capability* to compel its companies to follow its directions, it has the *opportunity* afforded by the presence of Chinese

AI-enabled products and services in our digital ecosystems, and it has demonstrated malign *intent* towards the democracies.

But this is a more subtle and complex problem than deciding whether to ban Chinese companies from participating in 5G networks. Telecommunications networks are the nervous systems that run down the spine of our digital ecosystems; they're strategic points of vulnerability for all digital technologies. Protecting them from foreign intelligence agencies is a no-brainer and worth the economic and political costs. And those costs are bounded because 5G is a small group of easily identifiable technologies.

In contrast, AI is a constellation of technologies and techniques embedded in thousands of applications, products and services, so the task is to identify where on the spectrum between national-security threat and moral panic each of these products sits. And then pick the fights that really matter.

What's the solution?

A general prohibition on all Chinese AI-enabled technology would be extremely costly and disruptive. Many businesses and researchers in the democracies want to continue collaborating on Chinese AI-enabled products because it helps them to innovate, build better products, offer cheaper services and publish scientific breakthroughs. The policy goal here is to take prudent steps to protect our digital ecosystems, not to economically decouple from China.

What's needed is a new three-step framework to identify, triage and manage the riskiest products and services. The intent is similar to that proposed in the recently introduced draft US RESTRICT Act, which seeks to identify and mitigate foreign threats to information and communications technology (ICT) products and services, although the focus here is on teasing out the most serious threats.

Step 1: *Audit*. Identify the AI systems whose purpose and functionality concern us most. What's the potential scale of our exposure to this product or service? How critical is this system to essential services, public health and safety, democratic processes, open markets, freedom of speech and the rule of law? What are the levels of dependency and redundancy should it be compromised or unavailable?

Step 2: *Red Team*. Anyone can identify the risk of embedding many PRC-made technologies into sensitive locations, such as government infrastructure, but, in other cases, the level of risk will be unclear. For those instances, you need to set a thief to catch a thief. What could a team of specialists do if they had privileged access to (that is, 'owned') a candidate system identified in Step 1—people with experience in intelligence operations, cybersecurity and perhaps military planning, combined with relevant technical subject-matter experts? This is the real-world test because all intelligence operations cost time and money, and some points of presence in a target ecosystem offer more scalable and effective opportunities than others. PRC-made cameras and drones in sensitive locations are a legitimate concern, but crippling supply chains through accessing ship-to-shore cranes would be devastating.

For example, we know that TikTok data can be accessed by PRC agencies and reportedly also reveal a user's location, so it's obvious that military and government officials shouldn't use the app. Journalists should also think carefully about this, too. Beyond that, the merits of a general ban on technical security grounds are a bit murky. Can our Red Team use the app to jump onto connected mobiles and IT systems to plant spying malware? What system mitigations could stop them getting access to data on connected systems? If the team revealed serious vulnerabilities that can't be mitigated, a general ban might be appropriate.

Step 3: *Regulate*. Decide what to do about a system identified as 'high risk'. Treatment measures might range from prohibiting Chinese AI-enabled technology in some parts of the network, a ban on government procurement or use, or a general prohibition. Short of that, governments could insist on measures to mitigate the identified risk or dilute the risk through redundancy arrangements. And, in many cases, public education efforts along the lines of the new UK National Protective Security Authority may be an appropriate alternative to regulation.

The democracies need to think harder about Chinese AI-enabled technology in our digital ecosystems. But we shouldn't overreact: our approach to regulation should be anxious but selective.

Introduction

It seems like an age since we worried about China's dominion over the world's 5G networks. These days, the digital authoritarian threat feels decidedly steampunk—Russian missiles powered by washing-machine chips and stately Chinese surveillance balloons. And, meanwhile, our short attention spans are centred (ironically) on TikTok—an algorithmically addictive short video app owned by Chinese technology company ByteDance.

More broadly, there are widespread concerns that 'large language model' (LLM) generative AI such as ChatGPT will despoil our student youth, replace our jobs and outrun the regulatory capacity of the democracies.[2] To be sure, the way we trust and depend on AI to sustain and improve our lives is an experiment without precedent in human history. We rely on AI to make invisible decisions affecting our health, safety and wealth in critical public infrastructure and financial markets. Online, it shapes what we see, think, feel and choose. It knows more about us than we do ourselves, so it's handy for gatekeeping access to the things we want, such as jobs, welfare, credit and insurance. It calls out our transgressions when it calculates that we've committed fraud or traffic violations and it predicts our risk of committing criminal offences[3] and dying from disease. And now AI can generate complex text, images and code, which hitherto only humans could do, and do it in a fraction of the time.

So, understandably, many citizens and democratic governments are mistrustful about the impact of AI on our individual rights and economic security. Moves are afoot across the democracies to regulate AI, notably in the EU, which is poised to enact comprehensive AI regulations. In June 2023, the Australian Government also foreshadowed regulation to 'ensure the growth of artificial intelligence in Australia is safe and responsible'.[4]

But if we in the democracies are wary about AI, we should be even more circumspect about AI-enabled products and services from authoritarian countries that share neither our values nor our interests.

And, for the foreseeable future, that means the PRC. In the span of a generation, China has transfigured its technological base. Once barely capable of producing third-rate knock-offs of second-rate Soviet designs, it's now a peer tech competitor with the US in the field of leading-edge AI.[5] Kicked along by the search for technology to address the PRC Government's internal-security concerns, China's tech companies are now exporting their AI-enabled technology to the world.

Chinese AI-enabled products are price competitive and effective, which no doubt is why almost 1,000 Chinese-made surveillance cameras were installed across Australian Public Service agencies.[6] However, Chinese companies are also subject to the direction of the Chinese state.[7]

The challenge for democracies is how to manage the security risks posed by Chinese AI-enabled products and services. The underlying dynamic is the same as that which prompted concern over Chinese 5G vendors: the PRC Government has the *capability* to compel its companies to follow its directions, it has the *opportunity* afforded by the presence of Chinese AI-enabled products and services in our digital ecosystems, and it has demonstrated malign *intent* towards the democracies.

But this is a more subtle and complex problem than deciding whether to ban Chinese companies from participating in 5G networks. Telecommunications networks are the nervous systems that run down the spine of our digital ecosystems; they're strategic points of vulnerability for all digital technologies. Because of the nature of 5G technology, even extensive security mitigations can't shield sensitive data and network functions from vendors under instruction from Chinese security agencies.[8] Protecting these networks is a no-brainer and is worth the economic and political costs. And those costs are bounded because 5G is a small group of easily identifiable technologies.

In contrast, AI is a constellation of technologies and techniques embedded in thousands of applications, products and services, so the task is to identify where on the spectrum between national-security threat and moral panic each of those products sits. And then pick the fights that really matter.

This report is broken down into six sections. The first section highlights our dependency on AI-enabled products and services. The second examines China's efforts to export AI-enabled products and services and promote its model of digitally enabled authoritarianism, in competition with the US and the norms and values of democracy. This section also surveys PRC laws compelling tech-sector cooperation and explains the nature of the threat, giving three examples of Chinese AI-enabled products of potential concern. It also explains why India is particularly vulnerable to the threat.

In the third section, the report looks at the two key democratic responses to the challenge of AI: on the one hand, US efforts to counter both China's development of advanced AI technologies and the threat from Chinese technology already present in the US digital ecosystem; on the other, a draft EU Regulation to protect the fundamental rights of EU citizens from the pernicious effects of AI. The fourth section of the report proposes a framework for triaging and managing the risk of China's authoritarian AI-enabled products and services embedded in democratic digital ecosystems. The final section acknowledges complementary efforts to mitigate the PRC threat to democracies' digital ecosystems.

What’s AI got to do with me?

You may not be interested in AI, but AI is interested in you. Today, you might have used AI to find the quickest route to a meeting through peak-hour traffic and, while you were using an AI-enabled search to find a decent podcast, driver-assist AI might have alerted you and applied the brakes just before you backended the car in front, which had braked suddenly to avoid the AI-powered numberplate-recognition system on the speed camera attached to the AI-controlled traffic lights powered by the AI-load-balanced electricity grid. In the aftermath, AI might have helped diagnose your detached retina, recalculate your safe-driving no-claim bonus and recommend a home-delivered pepperoni comfort pizza, which you ordered using your AI-enabled voice assistant and which, thanks to AI, was already in the oven of your local pizza chain in anticipation of your order.

You get the picture.

Digital technology, indeed many old technologies, such as cars and systems that monitor and regulate industrial processes and utilities, are increasingly underpinned by AI. Broadly, AI systems are ‘tools which allow computers to tackle specific problems that require skills normally only available to humans’.[9] The focus of this report in particular is AI defined as an ‘artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action’.[10] That is, the focus here isn’t on AI of itself, but products and services produced by Chinese companies that are enabled by AI.

Simple ‘expert system’ versions of AI might calculate the solution to a problem by following a set of rules (an algorithm) written for them by humans (such as basic automatic braking systems). More complicated ‘machine-learning systems’ automate that process, working out the rules for themselves by training on large datasets. By trial and error, they discover patterns in the data that provide the optimal solution to a particular problem (such as calculating traffic routes). The past decade has seen the rapid development of a branch of machine learning called ‘deep learning’, which can achieve superhuman performance tackling precise problems (for example, winning at chess or *go*) by applying, to large datasets, complex artificial neural networks that are inspired by the neurons in our brains.

And now ‘foundation model’ AI (of which LLMs are a subset) is upon us.[11] These generative AI systems, such as OpenAI’s GPT, can do many things really well by applying deep-learning techniques at scale to massive amounts of data to create outputs such as text, images and code. Foundation model AI is a step towards[12] ‘artificial general intelligence’ (AGI), which is ‘generally understood to mean AI capable of completing any intellectual task humans are capable of—in contrast to today’s ‘narrow’ AI, which is developed to complete a specific task’.[13] AGI and more tightly defined concepts such as ‘artificial superintelligence’ (ASI) and ‘transformative AI’ (TAI) are labels that are used to describe where AI is heading. They’re part informed speculation, part marketing. As such, they’re fuzzy, subjective and disputed.

AI multiplies the power of other technology. It’s as transformational to the modern world as ball bearings were to the machine age. And often about as glamorous.

AI is a broad church, and sales teams like to slap the AI label on anything with an ‘on’ switch. At the same time, as with all technology, what’s one day revolutionary is banal the next. Some pioneers in the field complain that, as soon as they get it working, they don’t call it AI anymore. This will no doubt soon apply to many applications of GPT (generative pre-trained transformer) technology. We’ll quickly get used to OpenAI’s GPT suite extending Bing searches, generating Excel spreadsheets and autocompleting coding on GitHub, and we’ll take it for granted.

What's the threat from Chinese AI-enabled technology?

If you think democracy is fragile, spare a thought for despots everywhere. To be one in any age is hard, thankless work. In the 21st century, it's terrifying. Modern technology challenges the business model of autocracy, particularly one like China built on the contradiction of a one-party state and a fiercely competitive capitalist economy. Markets are anarchic. People are suggestible. Enemies are everywhere. The arrival of the internet (a Western technology designed for frictionless global communication) facilitated the influx of foreign ideas (a worry for a country where twice last century such ideas led to revolution) and enabled citizens to spread unfiltered news and rumours and form spontaneous online communities.

At the same time, like a modern fly-by-wire fighter jet, authoritarian rule is inherently unstable, and effective governance requires constant realistic inputs to maintain its equilibrium. Without the messy, systemic self-correction forced on democratic governments by independent courts, open markets, unrestrained media and free elections, autocracies can lose sight of the terrain and fly into the ground. The Chinese Government's stubborn persistence with 'zero-COVID' measures and its rapid reversal following widespread protest is a case in point.[14]

For the Chinese Communist Party (CCP), AI-enabled technology offers a solution to the problem of disruptive or faulty inputs from below. It has rolled out integrated security technologies supported by AI and data analytics to surveil, measure and respond to potential sources of instability.[15] And its 'social credit' system, which seeks to reward and punish individuals, corporates and government entities, has a wider purpose to improve economic governance and service delivery. Think part government services portal, part financial creditworthiness agency, part government regulator, part frequent flyer program and part drivers-licence demerit-point program. AI promises to make possible the CCP's vision of 'data-driven governance'[16]—a more potent and ordered alternative to the tangled chaos of the democratic model—enabling 'different government organs [to] join hands to collect vast amounts of data within a coherent information ecosystem, across institutions, regions and administrative levels, as a basis for effective and responsive governance'.[17]

Beyond security and social-stability applications, the PRC Government also sees the economic benefits of AI. Indeed, Jeffrey Ding argues that this is 'the primary, immediate driving force behind China's development of AI … since AI systems could enable China to improve its productivity levels and meet GDP targets'.[18] Ding thinks that integrating AI systems into Chinese manufacturing and the like will help China overcome unfavourable demographic trends and escape the middle-income trap[19] whereby China grows old before it grows prosperous.

The ties that bind

Those efforts have given China a comparative advantage in the application of a range of AI-enabled technologies, especially those related to security and surveillance. As documented by ASPI, China's tech sector has benefited from state-security funding, permissive privacy protections and history's biggest sandbox to develop its wares.[20]

But the tech sector is also welded to the CCP by security laws, embedded party committees, 'golden shares'[21] held by the government and the threat of market intervention, detention and disgrace if founders get ahead of themselves.[22] In particular, the 2017 National Intelligence Law 'repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of "intelligence" work'.[23] As noted by Murray Scot Tanner and others, that law is part of 'an interrelated package of national security, cyberspace, and law enforcement legislation drafted under Xi Jinping … aimed at strengthening the legal basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them'.[24] Those include laws on Counterespionage (2014—recently strengthened[25]), National Security (2015), Counterterrorism (2015), Cybersecurity (2016) and Foreign NGO Management (2016), as well as the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016), and the Data Security Law (2021).

To be sure, most democracies also have laws enabling security and intelligence services to compel cooperation from private companies, but that access is enabled by legislation that's been debated and passed by elected representatives, and (as a generalisation) is limited to specific circumstances and overseen by varying combinations of independent inspectors, the courts and the parliaments themselves.

The AI struggle

Over recent years, China has exported its AI-enabled technology to the world, expanding its regional and global influence through 'smart city' technology initiatives and other digital infrastructure and connectivity agreements in its Digital Silk Road program (both part of the broader Belt and Road Initiative), as well as law-enforcement cooperation and training.[26] In technical standard-setting bodies and other international forums, China has sought standards that are advantageous to Chinese companies[27] and advocated its 'cyber sovereignty' internet governance model, which confers on government the right to 'delimit and control data flows based on its domestic security interests',[28] so that it might become 'an international consensus'.[29] For many authoritarian governments, the Chinese technology stack 'offers a plausible way for big, economically advanced countries to make their citizens rich while maintaining control over them'.[30]

It makes sense that the CCP would want to normalise and legitimise a technology model integral to its rule, but technological innovation has also become for Xi Jinping the 'main battlefield of the international strategic game'.[31] The contest between China's model of digital authoritarianism and liberal democracy has been likened to the competition between the democratic, fascist and communist social systems for much of last century.[32] Eric Schmidt, the former CEO of Google and chair of the 2021 US National Security Commission on Artificial Intelligence (NSCAI), believes that the 'AI revolution underpins the current contest of values between democracy and authoritarianism.'[33] The NSCAI itself notes that '[w]herever China controls the digital infrastructure, social media platforms, and e-commerce, it would possess greater leverage and power to coerce, propagandize, and shape the world to conform to its goals.'[34] Even those who are sceptical that China is exporting its governance model worry that its technology will place 'downward pressure … on democratic principles like transparency and accountability, particularly when it comes to the governance of surveillance technologies like facial recognition'.[35]

China is gaining rapidly in the race to develop and bring to market new AI technologies. Indeed, Eric Schmidt and Graham Allison warn that China 'stands today as a full-spectrum peer competitor of the United States in commercial and national security applications of AI'.[36] The NSCAI assessed in 2021 that, on current trends, 'China possesses the might, talent, and ambition to surpass the United States as the world's leader in AI in the next decade if current trends do not change'[37] (see box).

Who's winning the AI race?

In crude terms, sensors, data, algorithms and computing power are to AI what fat, salt, acid and heat are to cooking.[38] Data, sometimes fed by sensors, provides the ingredients, algorithms (with machine-learning techniques) the recipe and computing power the heat.

Sensors look like a win for China. Unrestrained by laws and norms, China's advances in sensors mean it can dominate much of the field in facial-recognition technology, for example. That permissive environment also gives China an unrivalled ability to collect and combine large, disparate datasets, leading one commentator to characterise China as the 'Saudi Arabia of data'.[39] However, that's misleading: unlike oil, 'data is not an all-purpose resource.'[40] Different AI systems call for 'distinct types of data' with unique 'type, structure, quality, and availability'. Hence, a country 'that first digitally stores, cleans, transforms, labels, and optimizes a set of data for specific projects—will be positioned to move faster toward its desired AI application, and hence at an advantage for that particular application'.[41] China's vast reserves of data may also be less of an advantage for generative AI because foundation models are 'trained on the much more voluminous unstructured data of the internet'.[42] But 56% of all websites are in English and only 1.5% are in Mandarin or China's other languages, and Chinese interaction with the internet is primarily through mobile super-apps such as WeChat and Weibo, which are 'walled gardens', largely unindexed by search engines.[43]

On computing power, specifically the microelectronics hardware on which all AI runs, the US retains a clear but diminishing lead in the design of advanced semiconductors (chips) and the technology underpinning their fabrication, although 'it is dependent on foreign supply chains and manufacturers in Asia that are vulnerable to coercion or disruption.'[44]

On algorithms / machine learning, it's a mixed picture with China and the US leading in different AI subdisciplines.[45] Given that human ingenuity is a proxy for innovation, the US's openness (relative to China) and its continued ability to attract top global AI talent gives it an advantage at a time when innovation is rapidly changing up the AI game.[46] It's no accident that the mobile phone was invented by the American son of Jewish immigrants from Ukraine. However, China excels at fast-following and scaling up, quickly bringing existing AI technology to market in areas such as speech recognition and fintech, and the largest of its hyperscaled consumer-facing platforms (Baidu, Alibaba and Tencent) rival Google, Amazon, Facebook and Microsoft,[47] so the challenge of regulating Chinese AI products and services will remain for the foreseeable future.

What, exactly, should we be worried about?

To reiterate: the concern here isn't China's AI capability *per se*. It's the integration of AI into products and services operated by PRC companies, which must cooperate with the Chinese state. As I've noted, AI is increasingly enabling all manner of pre-existing technologies, and China is skilled at integrating AI into commercial applications and offering them at competitive price points.

The core issue is this: notwithstanding the honourable intentions of individual vendors of Chinese AI-enabled products and services, they're subject to direction from PRC security and intelligence agencies. Against the background of growing strategic competition with China, can we trust that they'll protect our confidential information? Can we be sure their systems won't be manipulated to produce malign effects? And are we confident that they'll always be available when we need them?

We should worry about three kinds of Chinese AI-enabled technology:

- products and services (often physical infrastructure), where PRC ownership exposes democracies to risks of espionage (notably surveillance and data theft) and sabotage (especially disruption and denial of products and services)
- AI-enabled technology that facilitates foreign interference (malign covert influence on behalf of a foreign power), the most pervasive example being TikTok
- LLM AI and other emerging generative AI systems—a future threat that we need to start thinking about now.

This report is focused on the first category (and indeed looks at TikTok through the prism of espionage and sabotage), but, when we think about how we might manage Chinese AI-enabled technology, we should consider all of them.

In all three cases, the vector for this harm is cyberspace—our digital networks, but it's a particular form of cyber activity. This isn't about malicious cyber actors hacking into networks from the outside, but 'legitimate' actions taken by PRC companies on their own networks within our digital ecosystems at the direction of the Chinese state. Those actions might be triggered remotely or (wittingly or unwittingly) by service staff updating system software. This capability gives Chinese security services a sizable asymmetric advantage in one of the biggest problems facing intelligence operations the world over: how to gain access to protected networks.[48]

As with Chinese 5G kit, the issue isn't whether there's a 'smoking gun' proving that Chinese AI-enabled products and services have already taken such actions at the behest of the CCP's security services. The concern is a 'loaded gun' within our digital ecosystems. The question is: how much risk are we willing to bear against the background of growing strategic tensions with China?

The following section contains three examples of the potential for harm to the democracies. The section after it briefly surveys the particular risks to India's critical infrastructure posed by Chinese AI-enabled technology.

Security concerns about PRC AI-enabled technology

Ship-to-shore cranes

In March this year, the *Wall Street Journal* reported that the Chinese company Shanghai Zhenhua Heavy Industries Co. Ltd (ZPMC) controls around 70% of the global market for cranes.[49] Offering good-quality cranes that are significantly cheaper than Western models, the company has sold cranes to more than 100 countries. It reportedly makes 80% of the ship-to-shore cranes in use in US ports, and its cranes are installed at Sydney's Port Botany as well as ports in Brisbane, Melbourne and Fremantle, Western Australia.[50]

In a 2017 video, ZPMC's then-chairman Hailiang Song explained that 'We used to sell hardware, and now we are selling software and service.' The accompanying article on Microsoft's website explains that 'ZPMC is leveraging the Microsoft Cloud to build an Internet of Things platform that connects equipment, analyzes real-time data and informs a global monitoring hub. The company is integrating machine learning and advanced analytics for predictive maintenance and building remote monitoring, servicing and operations systems that boost efficiency, safety and customer satisfaction.' In the video, a company official explains that 'Through our main office in Shanghai, you can monitor all the cranes and help them solve the problem. No need to fly from Shanghai to everywhere!'[51] US officials reportedly told the *Wall Street Journal* that in some cases the cranes are supported by Chinese nationals working on two-year US visas.

So, on the face of it, those cranes could be accessed remotely or by servicing staff. What could China do with that? According to the paper, the US Defense Intelligence Agency concluded in 2021 'that Beijing could potentially throttle port traffic or gather intelligence on military equipment being shipped'. Noting that '[i]t wouldn't be hard for an attacker to disable one sensor on a crane and prevent the crane from moving,' a former head of cybersecurity for the port of Houston observed that '[t]hese systems aren't designed for security, they are designed for operations.'[52] Which is unfortunate, because the cranes reportedly also 'contain sophisticated sensors that can register and track the provenance and destinations of containers, prompting concerns that China could capture information about materiel being shipped in or out of the country to support US military operations around the world.'[53] One former Pentagon official has noted that 'because US military logistics organizations must share information with a wide variety of commercial businesses with inconsistent cybersecurity, these networks are uniquely vulnerable to enemy attacks.'[54]

Screening equipment

In 2020, the *Wall Street Journal* also reported US concern that Nuctech Co. Ltd, a world-leading producer of screening and inspection equipment with close links to Chinese state-owned enterprises, had secured a 90% share of Europe's sea-cargo screening equipment market and up to 50% of the market for airport passenger baggage and cargo screening, not least because its products were 25%–50% cheaper than those of its competitors.[55] With factories in Poland and Brazil, the company claims that it exports equipment, systems and services to 170 countries.[56]

Biometrics, data and AI are central to the company's products.[57] According to 2020 ASPI research, Australian state and federal government departments have invested heavily in Nuctech equipment and services since the Australian Customs Service's first order in 2001.[58] Nuctech systems are installed at major ports and some airports, and the company has contracts with state governments to provide and maintain body scanners at prisons and courts.[59] There's no evidence that these particular systems can be or, to date, have been maliciously manipulated either remotely or by servicing personnel. And it remains unclear to what extent Nuctech services connect with national border-control and customs databases, including passenger identification systems.[60] The company denies that it has any access 'whatsoever' to data generated by Nuctech products.[61]

Yet security concerns persist. The US banned Nuctech from its airports in 2014 following a classified review by the Transportation Security Administration and, in 2020, added the company to its banned entity list 'for its involvement in activities that are contrary to the national security interests of the United States'. In the same year, due to security concerns, Canada reversed a decision to buy Nuctech scanners for its 170 overseas diplomatic missions.[62]

In relation to Europe's reliance on Nuctech, the *Wall Street Journal* noted that '[s]ystems that screen cargo at ports and checked baggage at airports and railway stations are increasingly linked up to databases with shipping manifests and passenger information, including passports, fingerprints and other details'—potentially a trove of personal, commercial and military logistics information.[63] The company has reportedly supplied cargo scanners along Finland's border with Russia, the EU's borders with Belarus, Ukraine and Kaliningrad (Russia's Baltic Sea territory) and a nuclear-missile storage site between Lithuania and Poland. Given China's strategic alignment with Russia and its 'pro-Russian neutrality' in relation to the invasion of Ukraine, this is a concern.

In connection with the Canadian scanning equipment, a senior Canadian cybersecurity official told a 2020 parliamentary inquiry that security-screening equipment and other types of equipment had evolved 'such that [they] could gather information that could be of risk to Canada'.[64] She explained that recent versions of security-screening equipment included 'embedded hard drives and USB ports that can be used for maintenance purposes, for uploading and downloading data and software updates'. She added that the problem is 'whether there are any additional capabilities embedded within the machinery that are of concern'.

Digitised railway networks

In March this year, *Reuters* reported that Germany's state-owned Deutsche Bahn, one of Europe's largest rail networks, had selected Huawei to build a network to form the backbone of its new digital infrastructure, which will enable it to 'remotely steer' all its operations.[65] *Reuters* cited claims by Huawei critics that 'close links to China's security services means that the use of its technology could give Chinese spies and even saboteurs access to swathes of essential infrastructure' and that, according to cybersecurity experts, the switches and routers supplied by Huawei under the contract 'contain software that needs to be regularly updated remotely, potentially allowing for malicious updates'. Similar concerns were raised when, in 2019, Huawei reportedly undercut its rivals by 50% to win a contract to deliver a new digital signalling system to Brisbane's Cross River Rail Authority. The rail network reportedly carried 55 million passengers a year and controlled the movement of freight trains carrying goods to and from the port of Brisbane.[66] Huawei also supplies the digital radio systems for Sydney's rail transit system.[67]

Huawei appears to be investing heavily in AI solutions for digitised railway networks. Information on its website published in 2021 explains that 'Huawei is supporting the rail industry in its efforts to digitalise, particularly in the areas of connectivity, cloud infrastructure and artificial intelligence, in order to improve operational efficiency and customer satisfaction.'[68]

A(I) passage to India?

The risk to democracies' digital ecosystems is commensurate with the PRC's strategic ambitions. In general, the closer democracies are to the PRC, the more immediate the threat. Japan[69] and South Korea should be vigilant, but India even more so, for two reasons. First, India is industrialising and modernising rapidly, so price-competitive, effective Chinese gear will be a tempting default first choice for its critical-infrastructure requirements, particularly in the absence of indigenous alternatives (which are more likely to be available to Japan and South Korea). Second, India has a border contested by China, a neighbouring nuclear power. For India, this is a ground game with trigger fingers, so perhaps the regulation threshold should be lower for India.

We already know that India's critical infrastructure is a target for Chinese intelligence agencies. In February 2021, *Recorded Future*'s Insikt threat research division revealed that PRC cyber threat actors targeted two seaports and 'a large swathe of India's power sector', including four of the five regional load despatch centres responsible for balancing electricity supply and demand, in 'a concerted campaign against India's critical infrastructure'. Insikt assessed that those intrusions posed 'significant concerns over potential pre-positioning of network access to support Chinese strategic objectives … including geo-strategic signaling during heightened bilateral tensions, supporting influence operations, or as a precursor to kinetic escalation'.[70] In April last year, Insikt revealed that it had observed likely network intrusions targeting at least seven Indian state load despatch centres (SLDCs) 'responsible for carrying out real-time operations for grid control and electricity dispatch within these respective states'. Insikt noted that 'this targeting has been geographically concentrated, with the identified SLDCs located in North India, in proximity to the disputed India–China border in Ladakh.'[71]

To be clear: these were 'conventional' cyber intrusions from outside the network, but they reveal a malign PRC intent and the potential opportunity for cooperative PRC activity within AI-enabled products and services controlled by PRC vendors. Indeed, Indian commentators have warned of the risks of permitting Chinese companies to build power plants and core ICT and telecommunications networks in India.[72] The Indian Government appears to need no encouragement. In recent years, it has restricted Chinese investment and access to public procurement contracts and participation in critical infrastructure projects and has excluded Chinese companies from its 5G networks.[73] And, in probably one of its few touchpoints with the Taliban, the Indian Government has banned TikTok (and many other Chinese apps).[74]

How do we manage authoritarian AI technology?

Two key responses are emerging for countering the risks posed by AI to the democracies. Both are instructive for how the democracies might identify and manage authoritarian AI, the US model more so.

The EU draft AI Act defines the threats posed by AI in broad terms as a risk to individual rights, ethics and equality and proposes a country-agnostic regulatory framework to address those issues, whether the AI originates in the US or China. To be sure, there are similar efforts in the US to address AI, including by President Biden himself,[75] but his administration's main AI focus has been on countering authoritarian AI-enabled technology from China. For the US, China's growing AI capability is an economic and national-security threat, but also a threat to democracy and human rights. Indeed, echoing Xi Jinping, President Biden's Indo-Pacific Coordinator, Kurt Campbell, has referred to technology as 'the cutting edge arena of international competition in the period ahead, in the way nuclear missiles were … the defining feature of the Cold War'.[76]

The US approach

In response, the US is rolling out a wide-ranging suite of measures to maintain its competitive advantage, retard China's development of advanced computing technologies (essential for leading-edge AI) and slow the leakage of related high-end US expertise and intellectual property (see Appendix 'US efforts to constrain PRC advanced computing technologies in China and at home'). Those measures will certainly affect China's ability to compete in foundation model generative AI and emerging generative AI technologies, but they'll do little to manage the threat of PRC AI-enabled technology entering the market today.

To tackle this immediate challenge, a strongly bipartisan bill was introduced into the US Senate in early March this year. The Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act proposes a 'risk-based process, tailored to the rapidly changing technology and threat environment, by directing the Department of Commerce to identify and mitigate foreign threats to information and communications technology products and services'.[77] In his press release, one of the Act's key sponsors, US Senator Mark Warner (chairman of the Senate Select Committee on Intelligence), calls for 'a comprehensive, risk-based approach that proactively tackles sources of potentially dangerous technology before they gain a foothold in America, so we aren't playing Whac-A-Mole and scrambling to catch up once they're already ubiquitous'. The focus of the Act is clearly technology from China. The draft Act has been applauded by National Security Advisor Jake Sullivan, who has urged both Democrats and Republicans 'to act quickly to send it to the President's desk'.[78]

The summary of the bill sets out the challenge: 'Over the past years, foreign technology, including telecommunications equipment, social media applications, security software, and e-commerce platforms, have entered the US market and become increasingly embedded within our information and communications networks, posing novel threats to US citizens' data, US critical infrastructure, the privacy of Americans' and businesses' communications, our information ecosystem, and security of everyday products.'[79] In response, the Act would require the Secretary of Commerce to 'establish procedures to identify, deter, disrupt, prevent, prohibit, and mitigate transactions involving information and communications technology products in which any foreign adversary has any interest and poses undue or unacceptable risk to national security'. It prioritises the 'evaluation of information communications and technology products used in critical infrastructure, integral to telecommunications products, or pertaining to a range of defined emerging, foundational, and disruptive technologies with serious national security implications'. It mandates 'comprehensive actions to address risks of untrusted foreign information communications and technology products … identified by other government entities'. And it seeks to '[e]ducate the public and business community about the threat by requiring the Secretary of Commerce to coordinate with the Director of National Intelligence to provide declassified information on how transactions denied or otherwise mitigated posed undue or unacceptable risk'.[80]

While the immediate focus of the RESTRICT Act is TikTok, on face value it could apply to the full range of Chinese AI-enabled technology. Its implications are far-reaching and profound: for the US–China relationship; for their technological and economic decoupling; and for China's tech exports and development. It will also increase pressure on US allies and partners to follow suit.

The tech unravelling is a two-way street

In the flurry of recent US activity to manage the risks of Chinese technology, it's easy to forget that the travel has been in both directions. Indeed, China moved first. Since 2009, it has blocked Facebook, Google, Twitter and Instagram, as well as thousands of other foreign websites.[81] Its 2016 Cybersecurity and 2017 National Intelligence laws (and other statutes) place 'ill-defined and open-ended new security obligations and risks not only on US and other foreign citizens doing business or studying in China, but in particular on their Chinese partners and co-workers'.[82] And, since June 2020 (probably in response to bans on sales of US parts and technology to Huawei and other Chinese firms), China has required operators of 'critical information infrastructure' to go through a cybersecurity review process when ordering goods and services that may affect national security, which includes assessments of risks of supply-chain disruption due to 'politics, diplomacy and trade'.[83] At the time, the Cyberspace Administration of China denied that the rules were intended to restrict or discriminate against foreign companies.[84] However, in May this year, it announced that its review of products from Micron, the US's largest memory-chip maker, had found 'significant security risks' that would affect national security and warned operators of key Chinese information infrastructure—such as telecommunications firms and state-owned banks—against purchasing the company's goods.[85]

While the Micron review had been in train for almost two months, the timing of the announcement of its result was no accident, coming the day after a strongly worded G7 leaders' statement on economic resilience and economic security clearly aimed at reducing vulnerability to Chinese supply chains and economic coercion.[86] The statement underlines 'the importance of cooperating on enhancing security and resiliency in critical infrastructure particularly in the digital domain'. It notes the need for 'rigorous evaluation of equipment … to assess political, economic, and other risks of a non-technical nature posed by vendors and suppliers'. It expresses 'concern about regulations that unjustifiably require companies to localize data or those that allow governments to access data without appropriate safeguards and protections'. And it commits to 'deepen our strategic dialogue to seek to counter malicious practices in the digital sphere to protect global value and supply chains from illegitimate influence, espionage, illicit knowledge leakage, and sabotage'.[87]

The policy context for China's efforts to reduce its dependence on US and other foreign technology is Xi's push 'to achieve greater self-reliance and strength in science and technology', which was a key theme of his report to the CCP's 20th National Congress earlier this year.[88] This is as much about competing 'on the global frontiers of science and technology' as insulating China from US supply-chain countermeasures. For now, in any case, China will do what it can to exclude foreign technology and suffer what it must in the absence of domestic alternatives.

The EU approach

The EU's approach to managing the risks of AI is far broader than just countering authoritarian AI. The draft AI Act currently under consideration by the EU takes a first-principles approach to triaging the highest risk cases for regulatory attention across the vast field of *all* AI systems. Its purpose is to protect EU citizens from the risks of AI technology writ large—so that it's safe, trustworthy and accountable and doesn't discriminate against vulnerable groups due to unexplainable algorithmic bias. Like the EU's General Data Protection Regulation, the proposed AI Regulation is based on 'protecting human dignity and fundamental rights'.[89]

The draft Regulation separates AI products into four risk categories:[90]

1. 'Unacceptable risk' systems considered a clear threat to the safety, livelihoods and rights of people would be banned. Those include real-time biometric identification systems used in public places (with exceptions for law enforcement), social scoring by governments and the private sector, and AI systems that deploy harmful manipulative 'subliminal techniques' or exploit the vulnerabilities of a defined list of groups.

2. 'High-risk' AI systems would be subject to strict obligations before they can be put on the market (see below). This category currently includes products covered by EU health and safety laws that require third-party conformity assessment (such as medical devices, radio equipment, cars, toys and aviation equipment), as well as AI systems used for remote biometric identification, the regulation of road traffic, and water, gas, heating and electricity systems. Also covered are AI systems that make decisions on access to education, student assessment, recruitment, termination, eligibility for benefits and creditworthiness. Systems that dispatch emergency first-response services or have specific purposes in law enforcement, justice and immigration are also judged high risk. AI systems that merely supplement relevant decisions or actions (to be defined) are currently excluded from this category.

3. 'Limited risk' AI systems such as chatbots would require users to be aware that they're interacting with a machine so they can take an informed decision to continue or step back.

4. 'Minimal or no risk' AI systems, such as AI-enabled video games, spam filters and inventory-management systems, could be used freely.[91]

The steps required of vendors to comply with the draft Regulation are comprehensive. High-risk AI would need to be trained on datasets that are complete, representative and free of errors (to the best extent possible); implemented on traceable and auditable systems in a transparent manner; subject to human oversight at all times; and robust, accurate and secure. Before marketing such a system, operators would need to build a quality-management system, maintain detailed technical documentation and conduct an assessment to ensure that the system conforms to the Regulation (for certain systems, an external notified body will be involved in the conformity-assessment audit). Once their product is on the market, operators would need to monitor the system and update the documentation and conformity assessment if substantial changes are made. Significant penalties for violations would apply, particularly to large companies; for example, for noncompliance with banned AI systems, up to €30 million or 6% of global revenues, whichever is higher.

In May this year, two European Parliament committees recommended amendments to strengthen the draft Act, notably by imposing specific obligations on providers of foundation model generative AI, whether used on a stand-alone basis or embedded in an AI system or product. Notably, vendors would be expected to 'demonstrate through appropriate design, testing and analysis that [*sic*] the identification, the reduction and mitigation of reasonably foreseeable risks to health, safety, fundamental rights, the environment and democracy and the rule of law prior and throughout development'.[92] Vendors would also be obliged to 'process and incorporate only datasets that are subject to appropriate data governance measures for foundation models, in particular measures to examine the suitability of the data sources and possible biases and appropriate mitigation'.[93] The amendments were adopted by the European Parliament in mid-June; however, the final shape of the legislation will be determined through trilateral negotiations with the European Commission and Council of Ministers; officials are hoping for a deal by the end of the year.[94]

The proposed Regulation has been criticised for its ornate compliance burden, and, indeed, it reads like a musical notation system written by people who don't like music. The Centre for Data Innovation estimates that the regulation would deter investment in AI, impose enormous compliance costs, particularly on small and medium-sized enterprises, slow down the digitisation of the economy and encourage 'a brain drain of European entrepreneurs to countries where they can build AI companies with fewer bureaucratic hurdles than they face at home'[95]—a sort of reverse 'Brussels effect'.

One hundred and fifty of Europe's largest companies have reportedly written to the commission to complain that the draft legislation 'would jeopardise Europe's competitiveness and technological sovereignty'. They have particular concerns about the proposed restrictions on generative AI.[96] Recent Stanford Institute research has also warned that many of the foundation model providers, including OpenAI, Google and Meta, would 'not comply with [the European Parliament's proposed] requirements to describe the use of copyrighted training data, the hardware used and emissions produced in training, and how they evaluate and test models'.[97] (By contrast, in late March this year, the UK Government published an AI White Paper that proposes a more light-handed approach to regulating AI out of concern that 'rigid and onerous legislative requirements on businesses could hold back AI innovation'.[98])

That said, the draft EU framework has some attractive qualities. Principally, it provides a systematic approach to identifying AI systems that carry concerning risk. While the EU framework isn't designed with the risks of AI from digital authoritarian states in mind, the framework is a practical attempt to put arms around the totality of AI technology and identify which subtypes democracies should be worried about. The draft recognises that the EU can't and doesn't need to regulate everything (although the EU Parliament's version of the Act proposes to regulate *all* foundation AI, which would be a dramatic departure from this risk-based approach because it would assume 'that very broad categories of AI are inherently dangerous'.[99])

The EU scheme is also country-agnostic. Products would be banned or regulated on the basis of their functionality, not their provenance. The EU Regulation would theoretically capture and regulate the more pernicious types of AI from the US as well as from China. This has its advantages for countries hoping to avoid or minimise the kind of retaliation meted out to Australia when it called out 'high-risk' 5G vendors from China.

The downside of the EU Regulation is that it's breathtakingly ambitious and complex, with a load of implementation risk. And country-agnostic approaches sometimes distract from focusing on the most important threats.[100] Because it's trying to solve all the AI problems in one go, applying it to authoritarian AI could be a bit like renovating your kitchen while re-roofing your house: it's possible in theory but it takes a lot of willpower.

And, while Europe is increasingly anxious about China's *de facto* support for Russia on Ukraine, it remains conflicted about China. Certainly, willpower to confront PRC digital-security risks has been lacking in the past. EU members have been slow to ban Huawei from their 5G networks[101] and quick to penalise US big tech under the General Data Protection Regulation,[102] as demonstrated by the recent record US$1.3 billion fine handed out to Meta for sending Facebook user information to the US due to EU regulator concern that it can be accessed by US intelligence agencies beyond effective legal challenge.[103]

There are signs that Europe is shifting on China. In a tough speech on the eve of her visit with French President Macron to China in April this year, European Commission President Ursula von der Leyen noted that Chinese companies 'are obliged by law to assist state intelligence-gathering operations and to keep it secret' and that the CCP's 'clear goal is a systemic change of the international order with China at its centre'.[104] In mid-June, the commission announced that it would phase out its procurement and contracts with Huawei and ZTE and urged member states 'to adopt urgently relevant measures as recommended in the EU [2020 5G cybersecurity] Toolbox, to effectively and quickly address the risks posed by the identified suppliers'.[105]

And, in late June, the commission released a European economic security strategy in response to '[r] isks presented by certain economic linkages [which are] evolving quickly in the current geopolitical and technological environment and are increasingly merging with security concerns'.[106] The strategy seeks to preserve 'the vast majority of Europe's highly valuable economic links to the world while ensuring that the new risks we face, which are narrow but critical, are effectively tackled'.[107] The strategy focuses on the risks of 'certain economic linkages' (code for China) in four areas: the resilience of supply chains; risks to the physical and cybersecurity of critical infrastructure; risks related to technology security and leakage; and risks of weaponisation of economic dependences or economic coercion. It proposes multiple measures to tackle those risks, some of which would help address the concerns raised in this paper.

Of course, the power to take action rests with EU countries, and its two leading members, France and Germany, are wobbly on China. To be sure, both countries signed off on the 'G7 leaders' statement on economic and economic security', which takes aim at Chinese supply chains and economic coercion, in May this year.[108] Against that, among the things traded by Macron on his trip to China in return for business deals and Xi's blandishments on Ukraine was a promise 'to continue to process licensing applications from Chinese companies in a fair and non-discriminatory manner on the basis of the laws and regulations of the two countries, including national security'.[109]

Germany's views on China are more interesting. The government's recently-released Strategy on China[110] brings German views on China closer to the European Commission's.[111] But the issue of Chinese technology appears to be heavily contested by the business community and within the coalition government—with resulting mixed messages. On the one hand, it was reported in March this

year that Germany's cybersecurity agency is preparing to ban new Huawei and ZTE equipment from the country's 5G networks, which are heavily dependent on Chinese 5G equipment.[112] Also, reportedly, residual Chinese telco kit is under review, and German agencies are also looking at expanding scrutiny to other kinds of technology from authoritarian countries.[113] On the other hand, in February this year, ZTE announced that Germany had certified its 5G radios[114] and, as I've noted, in March this year German rail operator Deutsche Bahn chose Huawei to build the network underpinning its digital infrastructure.[115]

But there's a deeper problem with the proposed EU AI Regulation: it's designed to deal with a challenge that's adjacent to but different from that posed by Chinese AI-enabled products and services. It's concerned with how to make AI 'human centric, so that people can trust that the technology is used in a way that is safe and compliant with the law, including the respect of fundamental rights'.[116] This is an important enterprise, but it's aimed at protecting the individual democratic rights of citizens, not the security of the democracies' digital ecosystem as a whole. Democratic countries must design AI regulations that address both those challenges, but they represent different kinds of risk.

And they require distinct approaches. The EU Regulation has a different starting point from that required for the authoritarian challenge. The EU assumption is that appropriately regulated vendors can be trusted if they meet the rigorous and ongoing compliance regime, on pain of reputational damage and stiff financial sanctions for breaches. However, in a digital world where systems can be invisibly manipulated remotely or directly through vendor servicing contracts, can this approach ensure that PRC companies under pressure from their security services won't make their products and services available as a covert platform for Chinese influence, espionage and sabotage?

Finding the right balance between national-security threat and moral panic

For a number of practical reasons, not least the sheer breadth and variety of AI-enabled technology, there should be a high benchmark for regulating Chinese AI-enabled technology. Regulation increases economic costs for affected businesses, public utilities and research organisations. Many businesses and researchers in the democracies want to continue collaborating on Chinese AI-enabled products because it helps them to innovate, build better products, offer cheaper services and publish scientific breakthroughs. Collaboration with a Chinese self-driving car company with access to large volumes of training data might be the competitive edge for a tech start-up founder in Silicon Valley who's building self-driving cars. Access to cheaper cranes and container-scanning equipment from China may make Australian ports more economically viable. Chinese body-scanning equipment may be a significant but affordable security upgrade for Indian prisons. A medical scientist in the UK researching AI to detect brain tumours might rely on a world-leading Chinese medical AI system.

The regulation of Chinese products would also tend to disadvantage low-income consumers. That group can least afford the increased costs that would be passed on by companies forced to use higher cost non-Chinese products. There's also the risk of Chinese economic countermeasures against the smaller democracies, particularly if they go it alone.

The policy goal here is to take prudent steps to protect our digital ecosystems, not to economically decouple from China or weaken its tech exports (although both those will probably be second-order effects). Von der Leyen is right about China: we need to 'de-risk—not de-couple'.[117]

A framework to identify, triage and manage the risk of authoritarian AI-enabled products and services might consist of the three-step process set out below. The intent is similar to that proposed in the draft US RESTRICT Act, although the focus here is on teasing out the most serious threats.

Step 1: Audit

This report hasn't set out to provide comprehensive evidence that the democracies are riddled with Chinese AI-enabled products and services. The point is that no one has systematically looked. Some things, such as surveillance cameras, drones and TikTok, are obvious. Others, such as the cranes, security-screening equipment and digitised rail-signalling systems cited above emerge in the media from time to time. But, circumstantially, it's likely that there are many other examples that are less obvious. China is the world's second largest economy, with a vast industrial and technological base that produces industrial and consumer goods and services at highly competitive prices. At a minimum, it's worth understanding the level of exposure.

An audit should identify AI-enabled systems the purpose and functionality of which warrant closer inspection. What's the potential scale of our exposure to this product or service? Where is it or could it be deployed? What groups and how many people are or might be affected? How critical is this system to essential services, public health and safety, democratic processes, open markets, freedom of speech and the rule of law? What are the levels of dependency and redundancy should it be compromised or unavailable?

A good place to start looking are sectors in which PRC intrusions have been detected, since that's a decent indicator of PRC security agencies' interest. It's instructive that attacks attributed by Microsoft in late May this year to Volt Typhoon, 'a state-sponsored actor based in China', have since 2021 'targeted critical infrastructure organizations in Guam and elsewhere in the United States [spanning] the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors'.[118]

As I've noted, the EU's risk-based categories are a useful model. However, given that the object of regulation here isn't companies seeking to maximise their profits while guarding their reputations but companies vulnerable to direction by the covert arm of a state actor, logically many products and services classed by the EU as 'high-risk' (acceptable with mitigation) or even 'minimal or no risk' (no further action) may require a stronger response. It's one thing to regulate and trust a 'high-risk' AI-enabled Siemens SCADA[119] system to control your road traffic, water, gas, heating and electricity systems, but it might be more prudent to ban an equivalent Chinese system. The EU framework rates inventory-management systems as 'minimal or no risk', but, having lived through a pandemic, we all understand the importance of supermarket inventory systems, so we should also regard PRC inventory products more warily.

AI-enabled products and services evolve rapidly. As their capabilities improve, so may their risk profile, so the audit/review process needs to be ongoing.

One final point. Identifying products made in China isn't straightforward. In response to mounting suspicion towards PRC products, many Chinese companies don't flaunt their origins. A recent review by *The Economist* of dozens of Chinese companies' websites found that most could easily pass for Western brands.[120] And some products that are claimed to be made in third countries may be entirely composed of PRC components under the skin. A 2022 investigation by Taiwan's *CommonWealth Magazine* into a 'made in Taiwan' Benelink video surveillance camera discovered that 'From the external structure to the internal motherboard, it is exactly the same as the products of China's Hikvision', which is banned in the US and prohibited for use by Taiwanese public agencies (and now, it seems, by federal agencies in Australia).[121] The central question is: are these products and services able to be interfered with by a company that can be directed by the Chinese state? For this sort of problem, we need a second step.

Step 2: Red Team

Anyone can identify the risk of many PRC-made AI-enabled technologies in sensitive locations such as government infrastructure, but, in other cases, the level of risk will be unclear. In such cases, you need to set a thief to catch a thief. The best gamekeepers are those who can get inside the poacher's mind. A team of people with experience in intelligence operations, cybersecurity and perhaps military planning, combined with relevant technical subject-matter experts, could provide valuable insights to identify the devices, systems and use cases we should really be concerned about. This overlaps with but is broader than a purely cybersecurity approach. It's less about whether the product or service contains vulnerabilities or suspect code and how we might defend against that. Rather, it's about how we could attack an adversary using the 'legitimate' functionality in the vendor's system to conduct harmful operations.

What could our agencies and militaries do if they had privileged access to (that is, 'owned') a candidate AI-enabled system identified in Step 1? This is the real-world test because all intelligence operations cost time and money, particularly the useful sort that are integrated into a broader plan involving other instruments of national power, such as the armed forces. Just because the PRC security services can compel the cooperation of any Chinese company doesn't mean they will. Their legally sanctioned ubiquity of access provides many options, but these are very busy people with full days. Some points of presence in a target ecosystem offer more opportunities than others. PRC-made cameras and drones in sensitive locations are a legitimate concern, but their usefulness may be localised and not scalable. However, effects in narrow areas such as electricity grids and fuel-distribution and logistics systems could be devastating.

The level of threat isn't always self-evident. Some Chinese kit that appears dubious might not, in practice, be a useful vector for nefarious operations. Surveillance cameras and cranes stick out like balloons, but their risk depends on where they are and what they're connected to. Is there a pathway back to China or backdoor access to other networks of interest? Can that risk be mitigated, or should there be a blanket ban?

What could our security and intelligence agencies do with TikTok if they could compel the company to fully cooperate in intelligence operations? TikTok reportedly harvests more data than other social-media apps, including detailed information about the user's location and other apps that they're running (which presumably is why it provides such a satisfying user experience).[122] We know that data can be accessed by PRC agencies, so government and military folk should certainly not be using TikTok. Indeed many governments (including Australia's) have already banned the app from official devices.[123] And any journalist who recalls encoding their sources in a little black book and vehemently opposing their government's surveillance laws might want to toss TikTok.

Beyond that, the merits of a general ban on *technical security grounds* (instead of the long-term impact of young minds shaped by its curated content) are a bit murky, so 'red team' analysis might be useful. Can our Red Team use the app to jump onto connected mobiles and IT systems to plant spying malware? And what data can TikTok harvest from government and commercial websites carrying TikTok tracking pixels?[124] US Federal Bureau of Investigation Director Christopher Wray has noted the risk to connected systems: 'They have the ability on it to get … access to the software to devices. So you're talking about millions of devices and that gives them the ability to engage in different types of cyber activity through that.'[125] What system mitigations could stop us getting access to data or onto connected systems if we had compelled access to TikTok systems? If the Red Team revealed serious vulnerabilities that could not be mitigated, a general ban might be appropriate.

One other thing: the all-clear for any app is only good for that version of the software. We're always potentially one update away from more pernicious capabilities. Thus, the price of (teenage) freedom is eternal vigilance on TikTok.

The scale of the Red Team undertaking suggests a division of effort among the democracies, starting with the Five Eyes. That collaboration could then be expanded to other democracies—notably Quad members Japan and India, which have a particularly strong incentive to understand the risks of Chinese technology, given their geography.

Advice from security and intelligence agencies has credibility because, having hunted with the hounds, they know best how to protect the hares. This approach is reflected in the UK security service's (MI5's) new National Protective Security Authority, which will 'provide expert, intelligence-led advice [and training] to businesses and institutions in sensitive sectors of the economy, including critical infrastructure, emerging technology and academia'.[126] That decision partly reflects the UK Government's intent to 'strengthen our national security protections in those areas where the actions of the CCP pose a threat to our people, prosperity and security', including in critical national infrastructure and supply chains.[127] The UK Government has also foreshadowed a UK Supply Chains and Import Strategy 'to support specific government and business action to strengthen our resilience in critical sectors'.[128]

Step 3: Regulate

Decide what to do about a system identified as high risk. Treatment measures might range from prohibiting Chinese AI-enabled technology in some parts of the network, to a ban on government procurement or use, or to a general prohibition. Short of that, governments could insist on measures to mitigate the identified risk or dilute the risk through redundancy arrangements. For example, some US ports with ZPMC cranes reportedly use software provided by a Swiss company to operate the cranes.[129]

The levels of risk and treatment need to be case-specific. Should US hospitals continue to use PRC company UBTECH Robotics' ADIBOT-A autonomous UV-C disinfection robots with AI featuring multiple

radar and mapping technologies?[130] Probably. Is it a good idea for a nuclear facility to use UBTECH's ATRIS all-terrain security patrol robot for intelligent security with binocular cloud-based camera capabilities and built-in sensor technology including infrared and facial equipment?[131] Perhaps not. Should DJI drones be used by our militaries and border control authorities? Reputational risks aside, that depends on what they're used for and how well they can be secured (see 'Step 2: Red Team').[132] Is there an equally compelling case that DJI drones shouldn't continue to be available to consumers? Doubtful.

As the Brits understand, public education about the risks is also key, and in many cases may be an appropriate alternative to regulation. For example, short of fully banning TikTok, governments could alert citizens to the platform's censored feed and the risks to their data.

Wherever they can, the democracies should regulate in unison, not least because collective regulatory responses from like-minded countries are less likely to lead to Chinese retaliation because they raise China's reputational and economic costs.[133]

A new framework to regulate PRC-made generative AI

The foregoing three-step framework could be used to regulate PRC-made LLMs and other generative AI. Baidu, Alibaba, Huawei, SenseTime and other Chinese companies are developing products similar to ChatGTP.[134] It's early days, but a couple of observations are possible. At its broadest level, generative AI churns through vast inputs of text, image, audio and video data to produce outputs that are useful because they reflect reasonably accurate information about the world. In the same way that the democracies worry about generative AI's impact on citizens' rights, the CCP worries about what it means for authoritarian rule. It's a challenge for the party, up there with regulating the internet, but with sharper costs for getting the balance wrong. How can the CCP control this new information environment without damaging China's bid for leadership in generative AI technologies?[135]

There's a question about whether an LLM that was acceptable to China's regulators would be commercially competitive in the democracies. As *The Economist* has put it, 'it is difficult to see how a Chinese company could create something as wide-ranging and human-like (ie, unpredictable) as ChatGPT while staying within the government's rules.'[136] If we apply to Chinese LLMs the same ethical standards we use to measure LLMs developed in the democracies, one wonders about the attractions of a product that conforms with rules that it 'not subvert state power, incite secession, harm national unity or disturb the economic or social order [and] be in line with the country's socialist values'?[137]

But history suggests that we shouldn't underestimate China's ability to thread this needle. If LLMs and other generative AI are rendered safe for the CCP, we should be sceptical about whether they're safe for the democracies. The old adage is 'rubbish in—rubbish out', so, in tandem with understanding how we protect our individual rights from this kind of AI, we need to start thinking about how we protect our digital ecosystems from its authoritarian analogues.

Other pieces of the puzzle: standards, global partnerships and legal frameworks

The framework proposed here is a prudent step to address the problem posed by the presence of Chinese AI-enabled products and services, which are subject to direction from PRC security agencies, throughout the digital ecosystem of the democracies, but it's not a full solution.

As a number of commentators have pointed out, international standards that embed democratic digital norms into the technical specifications for AI products and services are also an important piece.[138] Regulating AI systems that have already been developed and deployed is reactive, difficult and time intensive. It's like building cybersecurity on top of an internet architecture designed for openness. And, because of the economic costs, lack of commercial alternatives and fear of trade retaliation, governments can be tempted to squint when regulating Chinese technology. Rather than banning those technologies, they may come up with mitigations that don't address all the underlying vulnerabilities. Clear, technically defined standards based on worst-case risks would be country-agnostic and create a market for alternatives to authoritarian products and services.

Of course, standards are most effective when developed early in the technology/product life cycle. We have an opportunity to do that now with LLMs and other emerging AGIs. This is where the two approaches to AI outlined in this report—one concerned with fundamental rights and the other with authoritarian AI from China—can work in harmony. Rules and norms designed to make emerging AI safe for democratic citizens are a good starting point for developing technical standards that would apply to all vendors—including those from authoritarian countries.

The US–EU Trade and Technology Council announced last December is a welcome effort to work together on the Joint AI Roadmap, which 'will inform our approaches to AI risk management and trustworthy AI on both sides of the Atlantic, and advance collaborative approaches in international standards bodies related to AI'.[139] As, too, is the G7's recent commitment to support standards to shape the next generation of technology based on 'our common democratic values and principles'.[140]

Standards probably won't solve the problem by themselves (Chinese companies might meet such standards and still enable their products and services as covert platforms for interference), but standards would reduce the magnitude of the problem and enable countries to exclude by default at least a portion of Chinese devices and services with undesirable functionality.

Another piece of the puzzle is legal frameworks obligating operators of critical infrastructure to protect their assets, which are potentially the vector for many of the highest threats to democracies' digital ecosystems from authoritarian AI. Those frameworks might be tightened up to compel operators to actively manage or limit their use of PRC AI-enabled products and services.[141]

We should also not forget that the ultimate goal is what Chris Inglis and Harry Krejsa call a 'durable and secure digital ecosystem'.[142] The approach advocated here to risk-manage exposure to Chinese AI-enabled technology won't stop China (or Russia) hacking into other non-cooperative networks to steal personal or intellectual property data or pre-position malware on critical infrastructure. But it would reduce a class of cyber threats from within AI-enabled products and services 'owned' by China in cases in which traditional cybersecurity defences aimed at managing intrusions from outside the network are likely to be less effective.[143]

Conclusion

The challenges posed by AI aren't new to the democracies, which have always needed to be vigilant about threats to both individual freedom and the security of the collective. Without either of those, democracies are imperilled. To be clear: prudent regulation is required to ensure that AI evolves to support the individual rights and prosperity of democratic citizens.

At the same time, democracies need to act to protect their digital ecosystems from authoritarian regimes that don't share their values or interests. The approach outlined here will be seen by some as dangerously extreme and by others as guilelessly cautious. It is, however, a balanced measure in a world in which China is neither at peace nor at war with us. We should be vigilant about the balloons in the sky, but we should think harder about the ghosts in the machine.

Appendix: US efforts to constrain PRC advanced computing technologies in China and at home

The proposed RESTRICT Act, with its focus on systematically regulating Chinese technology within the US digital ecosystem, raises the stakes in US–China tech rivalry.

However, US efforts to constrain China's tech rise have been building for some time. Indeed, growing bipartisan concern about China is a through line between the Trump and Biden administrations. President Trump placed hundreds of Chinese companies, organisations and affiliates on the Department of Commerce's Entity List, prohibiting them from buying parts and components from US companies without approval, including many of China's official 'AI champions', such as Huawei, iFlytek, Hikvision, Megvii Technology, SenseTime and Yitu. In 2020, Trump banned US companies and citizens from investing in the securities of dozens of Chinese technology companies and barred government procurement from a further subset. And, in the same year, Trump blocked the sale to Huawei of chips made abroad with US technology, crippling the company.[144]

US efforts to purge Chinese technology inside the US also reach back to the Trump administration as it sought ways to identify and remove suspect Chinese technology supplied by companies such as Huawei and ZTE. In 2018, Title 2 of the SECURE Technology Act created a federal council to analyse supply-chain security threats and recommended orders to remove or exclude certain technologies from federal networks. In 2019, the administration amended the National Defense Authorization Act to prohibit federal agencies from using equipment and services from five Chinese tech companies and working with contractors that use covered equipment. Also in 2019, the Department of Commerce was empowered to block public and private procurement and use of certain foreign ICT and services. And the 2020 Secure and Trusted Communications Networks Act permitted the Federal Communications Commission to restrict the purchase of certain ICT and systems using federal funds.[145] However, since many US public services and critical infrastructure systems are managed by state and local governments, implementation has been patchy and 'thus far, these entities have generally not revised their procurement laws to address those threats'.[146]

In October last year, President Biden extended Trump's approach, imposing wide-ranging export controls on the sale to China of advanced chips, chip-fabrication equipment, supercomputers and related software. Because those rules cover third-country suppliers that use US chip designs and tooling technology (pretty much all of them at the high end), they have the potential to severely impede China's advanced computing and AI development. As a further brake on China's catch-up efforts, the rules also prohibit US companies and citizens from sharing their expertise in those areas.[147] The administration is reportedly considering further measures to ban the export to China of even less capable AI chips and to restrict Chinese firms' use of US AI cloud services as a workaround.[148]

Also last September, Biden signed an executive order to strengthen US foreign investment screening to consider, in connection with countries of concern (read China), a new set of specific risk factors, such as 'whether a transaction impacts US leadership in technologies relevant to national security, or presents risks to US persons' data'.[149] And the administration is reportedly currently considering regulating US private-equity and venture-capital investment in Chinese companies involved in advanced semiconductors, quantum computing and some forms of AI that pose national-security risks.[150]

The Biden administration is also using industrial policy to maintain US technological leadership in the face of competition from China. In August 2022, Biden signed into law the CHIPS and Science Act, which is a bipartisan piece of legislation investing $280 billion to support US chip manufacture, research and development and STEM education and workforce-development initiatives.[151] The administration has also taken steps to protect US tech innovation from theft or abuse through Biden's May 2022 Executive Order on Improving the Nation's Cybersecurity and subsequent directives.[152]

Biden's National Security Advisor, Jake Sullivan, has framed those measures in a historical context. If the first wave of the digital revolution promised that new technologies would favour democracy and human rights, and a second wave saw an authoritarian counter-revolution, a third wave was needed 'to ensure that emerging technologies work for, not against, our democracies and security'.[153] Sullivan said it was no longer enough for the US to maintain 'relative' advantages over its competitors, making sure to stay a couple of generations ahead: 'Given the foundational nature of certain technologies, such as advanced logic and memory chips, we must maintain as large of a lead as possible.'[154]

This approach dramatically widens the target set from controlling weapons-related and dual-use technologies to a whole class of technology. The US now seeks to constrain Chinese supercomputing, AI and advanced chip production 'due to the enabling effects—rather than direct links—these technologies will have on China's military and surveillance capabilities'.[155]

The US approach has been criticised by those who argue that this 'economic iron curtain'[156] alienates Asian and European partners and allies,[157] harms US businesses and consumers, and won't work in the long run because the US lacks the overall dominance in dynamic advanced-technology supply chains.[158] Critics say that foreign companies will adapt workarounds 'designing-out' US technologies to evade US controls, leaving US companies with less revenue to innovate.[159]

However, the US's approach also plays to its strengths in computing power, leading-edge innovation and international partnerships,[160] all of which are areas where China faces challenges. And it pits a dynamic tech sector supported by directed government funding against a top-down party bureaucracy dictating priorities[161] to a deferential tech sector[162]—a game the US has won before.

Notes

1 Comment by then-Telstra CISO, Mike Burgess. Chris Player, ‘Telstra CISO: Cyber attacks are foreseeable events’, *ARN*, 3 June 2015, online.

2 For example, ‘Elon Musk is among 1,000 technology executives and experts who have called for an immediate pause in designing powerful artificial intelligence systems because of the fear they will “outsmart and replace us”.’ Mark Sellman, ‘Rein in AI before it outsmarts us all’, *The Times*, 29 March 2023, online.

3 Australian Human Rights Commission, *Human rights and technology, final report, 2021*, 43, online.

4 Ed Husic, ‘Safe and responsible AI’, media release, 1 June 2023, online.

5 Jamie Gaida, Jennifer Wong Leung, Stephan Robin, Danielle Cave, *ASPI’s Critical Technology Tracker: the global race for future power*, International Cyber Policy Centre, ASPI, Canberra, 2 March 2023, 20, online.

6 Ellen Whinnett, ‘Marles acts: Chinese cameras watching our top secret sites’, *The Australian*, 9 February 2023, online.

7 Murray Scot Tanner, ‘Beijing’s new National Intelligence Law: from defense to offense’, *Lawfare*, 20 July 2017, online; Bulelani Jili, *China’s surveillance ecosystem and the global spread of its tools*, Atlantic Council, October 2022, online.

8 Simeon Gilding, ‘5G choices: a pivotal moment in world affairs’, *The Strategist*, 29 January 2020, online.

9 GCHQ, ‘What is artificial intelligence?’, in *Pioneering a new national security: the ethics of artificial intelligence*, UK Government, no date, online.

10 This is part of a more comprehensive definition of AI contained in the 2019 US National Defense Authorization Act: ‘1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. 2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. 3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. 4. A set of techniques, including machine learning that is designed to approximate a cognitive task. 5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.’ John S McCain National Defense Authorization Act for Fiscal Year 2019, 1697–1698, online.

11 Center for Research on Foundation Models, *On the opportunities and risks of foundation models*, Stanford Institute for Human-Centered Artificial Intelligence, Stanford University, 16 August 2021, online.

12 Sébastien Bubeck, Varun Chandrasekaran, Ronen Eldan, Johannes Gehrke, Eric Horvitz, Ece Kamar, Peter Lee, Yin Tat Lee, Yuanzhi Li, Scott Lundberg, Harsha Nori, Hamid Palangi, Marco Tulio Ribeiro, Yi Zhang, ‘Sparks of artificial general intelligence: early experiments with GPT-4’, *arXiv*, Cornell University, 13 April 2023, online.

13 Henry A Kissinger, Eric Schmidt, Daniel Huttenlocher, *The Age of AI and our human future*, Little, Brown and Company, 2021, 88.

14 ‘By restricting the movement and freedom of hundreds of millions of Chinese citizens for almost three years, … Xi also fell into a trap. [L]acking effective feedback mechanisms, China’s top decision-maker evidently failed to realize the extent of public dissatisfaction until street protests erupted across major cities seven months later, calling for the zero-COVID program to end and even for Xi to step down.’ Yanzhong Huang, ‘China’s hidden COVID catastrophe: How Xi obscured a lethal viral wave—and what it means for the future of his regime’, *Foreign Affairs*, 16 February 2023, online.

15 Jili, *China’s surveillance ecosystem and the global spread of its tools*, 2–3; Dahlia Peterson, *Designing alternatives to China’s repressive surveillance state*, Center for Security and Emerging Technology, Georgetown University, October 2020, online.

16 Jessica Reilly, Muyao Lyu, Megan Robertson, ‘China’s social credit system: speculation vs reality: how far along is China’s much-hyped social credit system—and where is it heading next?’, *The Diplomat*, 30 March 2021, online.

17 Katja Drinhausen, Vincent Brussee, *China’s social credit system in 2021: from fragmentation towards integration*, Mercator Institute for China Studies, 9 May 2022 online.

18 Jeffrey Ding, *Deciphering China’s AI dream: the context, components, capabilities, and consequences of China’s strategy to lead the world in AI*, Centre for the Governance of AI, Future of Humanity Institute, University of Oxford, March 2018, online; ‘Forward thinking on China and artificial intelligence with Jeffrey Ding’, podcast, McKinsey Global Institute, 23 June 2021, online.

19 ‘The “middle-income trap” is a theory of economic development in which wages in a country rise to the point that growth potential in export-driven low-skill manufacturing is exhausted before it attains the innovative capability needed to boost productivity and compete with developed countries in higher value-chain industries. Thus, there are

few avenues for further growth—and wages stagnate.' 'China may be running out of time to escape the middle-income trap', Asia Society, no date, online.

[20] Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan, Elise Thomas, *Mapping China's technology giants*, ASPI, Canberra, 2019, online; Fergus Ryan, Danielle Cave, Vicky Xiuzhong Xu, *Mapping more of China's technology giants, AI and surveillance*, ASPI, Canberra, 2019, online; Fergus Ryan, Audrey Fritz, Daria Impiombato, *Reining in China's technology giants*, Issues paper, Report No. 46/2021, ASPI, Canberra.

[21] 'The government stakes are sometimes very small, like the 1% holding … in the digital-media unit of e-commerce giant Alibaba (and TikTok parent, Bytedance) … [b]ut they tend to give the government board seats, voting power and sway over business decisions'. Linking Wei, 'China's new way to control its biggest companies: golden shares', *Wall Street Journal*, 8 March 2023, online.

[22] After he criticised finance regulatory authorities in 2020, Alibaba co-founder, Jack Ma, was sidelined, reportedly spending most of his time outside China and ceding control over several of his companies. A major Chinese tech financier, Bao Fan, has also been detained by authorities since February this year without explanation. Linking Wei, 'China's new way to control its biggest companies: golden shares'.

[23] Tanner, 'Beijing's new National Intelligence Law: from defense to offense'.

[24] Tanner, 'Beijing's new National Intelligence Law: from defense to offense'; see also Jili, *China's surveillance ecosystem and the global spread of its tools*, 6.

[25] Laurie Chen, 'China approves wide-ranging expansion of counter-espionage law', *Reuters*, 27 April 2023, online.

[26] Katherine Atha, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, Emily Walz, *China's smart cities development*, report prepared on behalf of the US–China Economic and Security Review Commission, January 2020, online; Cave et al., *Mapping China's technology giants*; Ryan et al., *Mapping more of China's technology giants, AI and surveillance*; Ryan et al., *Reining in China's technology giants*.

[27] Atha et al., *China's smart cities development*, 58.

[28] Jili, *China's surveillance ecosystem and the global spread of its tools*, 3.

[29] Cave et al., *Mapping China's technology giants*, 8.

[30] Nicholas Wright, 'How artificial intelligence will reshape the global order: the coming competition between digital authoritarianism and liberal democracy', *Foreign Affairs*, 10 July 2018, online.

[31] Zichen Wang, 'Xi Jinping's speech on science & tech on May 28, 2021', *Pekingnology*, 9 June 2021, online.

[32] Wright, 'How artificial intelligence will reshape the global order: the coming competition between digital authoritarianism and liberal democracy'.

[33] Eric Schmidt, 'The AI revolution and strategic competition with China', *Project Syndicate*, 30 August 2021, online.

[34] National Security Commission on Artificial Intelligence (NSCAI), *Final report: National Security Commission on Artificial Intelligence*, US Government, 2021, 26, online.

[35] 'US–China technology competition: a *Brookings Global China* interview', *Brookings*, comment by Chris Meserole, December 2021, online.

[36] Graham Allison, Eric Schmidt, *Is China beating the US to AI supremacy?*, Belfer Center for Science & International Affairs, August 2020, 1, online.

[37] NSCAI, *Final report: National Security Commission on Artificial Intelligence*, 7.

[38] With apologies to Sameen Nosrat, *Salt, fat, acid, heat: mastering the elements of good cooking*, Simon & Schuster, 2017.

[39] Kai-Fu Lee, *AI superpowers: China, Silicon Valley, and the new world order*, Houghton Mifflin Harcourt, Boston, 2018. Although Paul Scharre notes that China's data probably lacks the diversity of that available to US companies, which have greater international reach; Paul Scharre, 'America can win the AI Race', *Foreign Affairs*, 4 April 2023, online.

[40] Husanjot Chahal, Ryan Fedasiuk, Carrick Flynn, *Messier than oil: assessing data advantage in military AI*, Center for Security and Emerging Technology, Georgetown University, July 2020, online.

[41] Chahal et al., *Messier than oil: assessing data advantage in military AI*.

[42] 'Just how good can China get at generative AI?', *The Economist*, 9 May 2023, online.

[43] 'Just how good can China get at generative AI?'.

[44] NSCAI, *Final report: National Security Commission on Artificial Intelligence*, 26.

[45] Gaida et al., *ASPI's Critical Technology Tracker: the global race for future power*, 23.

[46] '[H]alf of the world's AI's superstars work for US companies [and] America can recruit from all the world's 7.9 billion people, while inherent insularity restricts China to its own population'; Graham Allison, Kevin Klyman, Karina

Barbesino, Hugo Yen, *The great tech rivalry: China vs the US*, Belfer Center for Science and International Affairs / Harvard Kennedy School, December 2021, 13, online. And over half of all AI researchers working in the US are from abroad; Eric Schmidt, 'Innovation power: why technology will define the future of geopolitics', *Foreign Affairs*, 28 February 2023, online.

47 Allison et al., *The great tech rivalry: China vs the US*, 5–6.

48 Gilding, '5G choices: a pivotal moment in world affairs'.

49 Aruna Viswanatha, Gordon Lubold, Kate O'Keefe, 'Pentagon sees giant cargo cranes as possible Chinese spying tools', *Wall Street Journal*, 5 March 2023, online.

50 James Morrow, 'Chinese spy danger hiding in crane sight, say experts', *Daily Telegraph*, 6 March 2023, online.

51 'From connected cranes to remote controls, ZPMC is transforming shipping with smart port services', *news.microsoft.com*, no date, online.

52 Viswanatha et al., 'Pentagon sees giant cargo cranes as possible Chinese spying tools'.

53 Viswanatha et al., 'Pentagon sees giant cargo cranes as possible Chinese spying tools'.

54 Chris Dougherty, *Buying time: logistics for a new American way of war*, Center for a New American Security, April 2023, 9, online.

55 Kate O'Keeffe, Drew Hinshaw, Daniel Michaels, 'US presses Europe to uproot Chinese security-screening company', *Wall Street Journal*, 28 June 2020, online.

56 Kelsy Munro, Lin Li, 'Should Australia be buying border-security technology from China's Nuctech?', *The Strategist*, 17 December 2020, online.

57 Munro & Li, 'Should Australia be buying border-security technology from China's Nuctech?'. 'The company sells customs clearance passenger systems incorporating biometric identification, AI and other technologies' and it uses 'AI, big data and video analysis technologies to [automatically identify] high-risk passengers'; 'Port modernization, products and solutions', *Nuctech, Creating a Safer World*, archived. One of Nuctech's European managers has explained that 'AI algorithms will help security officials—airport and ports operators, customs authorities, government representatives—to efficiently analyze large amounts of data, ensure more accurate risk assessments and achieve higher security standards'; Robert Bos, Deputy Director-General, Nuctech Netherlands, 'Transparent, equal dialogue will lead to digital transformation', sponsored content, *Politico*, 29 October 2020, online. Nuctech's WEKNOW 100 AI inspection system 'is based on deep learning algorithm which enables the automatic recognition of various contrabands'. With the latest technology including image processing, pattern recognition and machine learning, 'the system can be widely used for x-ray scanners in subway, railway, highway, government agencies, logistics, courts, public security bureau, airports, exhibition halls and other places for security check'. 'NUCTECH™ WEKNOW100, AI inspection system', Nuctech Europe, *nuctecheurope.com*, online.

58 Munro & Li, 'Should Australia be buying border-security technology from China's Nuctech?'.

59 Nuctech's Australian website links to newspaper articles about the success of its body scanners at New South Wales's 'SuperMax' maximum-security prison and contraband found by (presumably its) scanning equipment at the Sydney Container Examination Facility: 'SuperMax guardian: Nutech HT series body-scanners block the smuggling of narcotics and contraband to Australia's worst criminals and terrorists'; 'Nearly 400kg of cocaine found hidden in an excavator, two men charged'; 'Ecstacy on the barbie: Australia seizes more than half a tonne of drugs smuggled in barbeques'; 'Ice worth $438m hidden in fridges: police'; 'Lifesaving find in NSW jail after full body scan'; online.

60 Munro & Li, 'Should Australia be buying border-security technology from China's Nuctech?'.

61 Bos, 'Transparent, equal dialogue will lead to digital transformation'.

62 Munro & Li, 'Should Australia be buying border-security technology from China's Nuctech?'.

63 O'Keeffe et al., 'US presses Europe to uproot Chinese security-screening company'.

64 Standing Committee on Government Operations and Estimates, *Ensuring robust security in federal purchasing*, House of Commons, Canadian Parliament, June 2021, 24, online.

65 Sarah Marsh, 'Exclusive: Deutsche Bahn bets on Huawei for railway digitalisation despite security concerns', *Reuters*, 11 March 2023, online.

66 Ben Packham, 'Huawei wins Brisbane railway signals contract', *The Australian*, 20 December 2019, online.

67 The NSW Government is apparently working to upgrade the digital network, which is reaching obsolescence; Tom Rabe, Olivia Ireland, Megan Gorrey, 'Premier apologises after train shutdown paralyses Sydney', *Sydney Morning Herald*, 9 March 2023, online.

68 Noting that 'as the physical railway network expands, it is not possible for humans to oversee it, let alone get a sense of the health of equipment and assets, or manage and schedule regular maintenance tasks', Huawei's website cites

a study predicting that AI ‘will play a fundamental role in applications such as rail automation, customer sentiment tracking, mobility health tracker, customer data engine and incident and disruption simulation [as well as] predictive asset maintenance, where AI will help inspect and maintain equipment before failures occur’. ‘Better rail services with digital transformation’, Huawei, 17 November 2021, online.

69 Indeed, in response to growing tension with China, in May last year Japan’s Diet passed the Economic Security Promotion Act, which, among other things, gives Japan’s government the ‘power to order companies to notify it of software updates and vet some equipment procurement in 14 industries, including energy, water supply, information technology, finance and transportation.’ Kaori Kaneko, Tim Kelly, ‘Japan passes economic security bill to guard sensitive technology’, *Reuters*, 11 May 2022, online.

70 China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions, Insikt Group, 28 February 2021, online.

71 Insikt Group, ‘Continued targeting of Indian power grid assets by Chinese state-sponsored activity group’, *Recorded Future*, 6 April 2022, online.

72 For example, Pavithran Rajan, ‘Chinese digital paw marks on India’s critical infrastructure’, *Policy Circle*, 1 March 2021, online; Sameer Patil, Kishika Mahajan, *Expanding Chinese cyber-espionage threat against India*, Observer Research Foundation, 18 April 2022, online.

73 Tanvi Madan, ‘China has lost India: How Beijing’s aggression pushed New Delhi to the West’, *Foreign Affairs*, 4 October 2022, online; Raj Verma, ‘India’s economic decoupling from China: a critical analysis’, *Research Gate*, January 2023, 150–153, online.

74 Most TikTok bans apply only to official devices, with the notable exception of the bans in India and Afghanistan; Aaron McDade, ‘Countries that have banned TikTok as US threatens nationwide ban’, *Business Insider,* 17 March 2023, online. See also Josh Taylor, ‘Australia-wide ban of TikTok on government devices announced as senior politicians quit the app’, *The Guardian*, 4 April 2023, online; Paayal Zaveri, ‘Why India banned TikTok—and what the US can learn from it, as pressure mounts for Biden to follow suit’, *Business Insider*, 7 January 2023, online.

75 US efforts in this area have been fragmented, and AI regulation has been largely limited to a patchwork of state laws. At the federal level, agencies such as the Federal Trade Commission and the Equal Employment Opportunity Commission are becoming more active, portending litigation risk for companies. And the White House’s Office of Science and Technology Policy is focused on the ‘sociotechnical’ risks of AI, announcing a ‘Blueprint for an AI Bill of Rights’ in October 2022. In late January this year, the US National Institute of Standards and Technology published an ‘AI Risk Management Framework’ for voluntary use by organisations designing, developing, deploying or using AI systems, which articulates the ‘characteristics that can make AI safe and secure, fair and accountable, and protective of our privacy’. Office of Science and Technology Policy, ‘Remarks of Dr Alondra Nelson at the launch of the NIST AI Risk Management Framework’, The White House, 26 January 2023, online. The Biden administration is also seeking public input on issues such as ‘standards, regulations, investments, and improved trust and safety practices’ to develop a national AI strategy to guide federal agencies—a move no doubt accelerated by emerging generative AI technology; Ryan Tracy, ‘Biden administration developing national AI strategy’, *Wall Street Journal*, 23 May 2023, online. And on 21 July, Biden announced that seven major US tech companies had signed up to voluntary commitments for responsible AI innovation, and he foreshadowed further executive action, legislation and regulation in this area; Remarks by President Biden on Artificial Intelligence, White House Briefing Room, 21 July 2023, online.

However, notwithstanding renewed congressional interest in AI regulation in response to generative AI, there’s little prospect of anything like the EU AI Regulation. Chanley T Howell, ‘AI regulation: Where do China, the EU, and the US stand today?’, Innovative Technology Insights, *Foley and Lardner LLP*, 3 August 2022, online; see also Daniel J Felz, Kimberly Kiefer Peretti, Alysa Austin, *Privacy, cyber & data strategy advisory*: *AI regulation in the US: What’s coming, and what companies need to do in 2023*, 9 December 2022, online.

76 The Hudson Institute, ‘Dialogues on American foreign policy and world affairs, a conversation with Kurt Campbell’, *YouTube*, 6 June 2023, online.

77 Mark Warner, ‘Senators introduce bipartisan Bill to tackle national security threats from foreign tech’, media release, 7 March 2023, online.

78 ‘Statement from National Security Advisor Jake Sullivan on the introduction of the RESTRICT Act’, The White House, 7 March 2023, online.

79 Mark Warner, John Thune, ‘Summary of the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act’, 7 March 2023, online.

80 Warner & Thune, ‘Summary of the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act’.

81 Li Yuan, ‘A generation grows up in China without Google, Facebook or Twitter’, *New York Times*, 6 August 2018, online.

82 Tanner, 'Beijing's new National Intelligence Law: from defense to offense'.

83 Yifan Wang, 'China toughens procurement rules for tech equipment, *Wall Street Journal*, 27 April 2020, online.

84 Wang, 'China toughens procurement rules for tech equipment'.

85 Lingling Wei, 'Beijing bans Micron as supplier to big Chinese firms, citing national security, *Wall Street Journal*, 21 May 2023, online.

86 'G7 leaders' statement on economic resilience and economic security', The White House, 20 May 2023, online.

87 'G7 leaders' statement on economic resilience and economic security'.

88 'Transcript: President Xi Jinping's report to China's 2022 party congress', *Nikkei Asia*, 18 October 2022 online.

89 Luciano Floridi, 'The European legislation on AI: a brief analysis of its philosophical approach', *Springer Link*, 3 June 2021, online.

90 The scope of the draft Regulation is evolving as it makes its way through the EU system, and it won't become law until at least later this year. For example, in December last year, the lists of unacceptable and high-risk AI were both broadened and narrowed by the EU Council. Laura De Boel, Wilson Sonsoni, 'Council of the EU proposes amendments to draft AI Act', 22 December 2022, online.

91 'Regulatory framework proposal on artificial intelligence', European Commission, 20 June 2023, online.

92 Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs, 'Compromise amendments on the draft report, proposal for a regulation of the European Parliament and of the Council on harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts', version 1.1, European Parliament, 16 May 2023', online.

93 Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs, 'Compromise amendments on the draft report, proposal for a regulation of the European Parliament and of the Council on harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts', version 1.1, European Parliament, 16 May 2023', online.

94 Luke Scanlon, Sarah Cameron, 'MEP's EU AI Act proposals focus on "foundation models"', *OUT-LAW*, Pinsent Masons, 16 May 2023, online; Kim Mackrael, 'AI regulation is here. Almost', *Wall Street Journal*, 14 June 2023, online.

95 Benjamin Mueller, *How much will the Artificial Intelligence Act cost Europe?*, Center for Data Innovation, July 2021, 3, online.

96 Javier Espinoza, 'European companies sound alarm over draft AI law', *Financial Times*, 30 June 2023, online.

97 Rishi Bommasani, Kevin Klyman, Daniel Zhang, Percy Liang, *Do foundation model providers comply with the draft EU AI Act?*, Center for Research on Foundation Models, Stanford University, 15 June 2023, online.

98 The paper, which seeks to address the same kinds of AI issues as the EU Regulation, proposes that AI principles would be implemented by existing industry regulators; Office of Artificial Intelligence, *Policy paper: A pro-innovation approach to AI regulation*, UK Department for Science, Innovation & Technology, 22 June 2023, online.

99 Ryan Browne, 'Europe takes aim at ChatGPT with what might soon be the West's first AI law. Here's what it means', *CNBC*, 15 May 2023, online.

100 Daniel Ward, *Losing our agnosticism: how to make Australia's foreign influence laws work*, ASPI, Canberra, 22 July 2021, online.

101 Laurens Cerulus, Sarah Wheaton, 'How Washington chased Huawei out of Europe', *Politico*, 23 November 2022, online.

102 See, for example, Omar Husain, '50 biggest GDPR fines and penalties so far (2023 version)', *enzuzo*, 15 December 2022, online.

103 Sam Schechner, 'Meta fined $1.3 billion over data transfers to US', *Wall Street Journal*, 22 May 2023, online.

104 'Speech by President von der Leyen on EU–China relations to the Mercator Institute for China Studies and the European Policy Centre', European Commission, Brussels, 30 March 2023, online.

105 'Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by member states', press release, European Commission, Brussels, 15 June 2023, online.

106 'An EU approach to enhance economic security', press release, European Commission, Brussels, 20 June 2023, online.

107 *European Economic Security Strategy*, European Commission, Brussels, 20 June 2023, online.

108 'G7 leaders' statement on economic resilience and economic security', European Council, 20 May 2023, online.

109 Finbarr Bermingham, @fbermingham, *Twitter*, 8 April 2023

110 Strategy on China of the Government of the Federal Republic of Germany, 14 July 2023, online.

111 Lily McElwee and Ilaria Mazzocco, *Germany's China Strategy marks a new approach in EU-China relations*, Center for Strategic and International Studies, 14 July 2023, online.

112 Oliver Moody, 'Berlin set to unplug Huawei from 5G', *The Times*, 7 March 2023, online.

113 William Boston, Bertand Benoit, 'Germany reviews 5G network safety, opening door to possible Huawei ban', *Wall Street Journal*, 7 March 2023, online. Germany passed legislation in 2020 enabling its government to ban telco vendors that make false declarations, refuse security audits or fail to properly divulge and address any security vulnerabilities in their products. In December last year, it was reported that the German Economic Ministry had a strategy paper recommending closer scrutiny of components that come from authoritarian states, including telco and IT equipment and products related to transport, water and food supply; Nick Wood, 'Germany gives ZTE's 5G kit the all-clear', *Telecoms.com*, 8 February 2023, online. And, in March this year, an Interior Ministry spokesperson told *Reuters* that the ministry was planning to expand current IT security legislation to cover more infrastructure and was working on a law strengthening cybersecurity; Sarah Marsh, 'Exclusive: Deutsche Bahn bets on Huawei for railway digitalisation despite security concerns', *Reuters*, 11 March 2023, online.

114 This product would be located in mobile towers on the edge of 5G networks. If this claim is true, it suggests that the German cybersecurity agency judged that its telcos could protect sensitive data in the core of their networks. Many other countries have concluded otherwise. Woods, 'Germany gives ZTE's 5G kit the all-clear'.

115 Marsh, 'Exclusive: Deutsche Bahn bets on Huawei for railway digitalisation despite security concerns'.

116 'Proposal for a Regulation of the European Parliament and the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts: Explanatory memorandum, 1.1 Reasons for and objectives of the proposal', *EUR-Lex*, 21 April 2021, online.

117 'Speech by President von der Leyen on EU–China relations to the Mercator Institute for China Studies and the European Policy Centre'.

118 Microsoft Threat Intelligence, 'Volt Typhoon targets US critical infrastructure with living-off-the-land techniques', *Microsoft Security Blog*, 24 May 2023, online.

119 Supervisory control and data acquisition systems are used for 'controlling, monitoring, and analyzing industrial devices and processes. The system consists of both software and hardware components and enables remote and on-site gathering of data from the industrial equipment. In that way, it allows companies to remotely manage industrial sites such as wind farms, because the company can access the turbine data and control them without being on site'. 'What is SCADA?', SCADA International, online.

120 'How China Inc is tackling the TikTok problem', *The Economist*, 8 March 2023, online.

121 Huang Yiyun, Huang Mingtan, 'China's Sky Eye becomes a Taiwanese quality good—dismantling the MIT surveillance system to tear open the truth of "Taiwan skin, mainland bones"', *CommonWealth Magazine*, 20 September 2022, translated by Jeffrey Ding, '"Taiwan skin, mainland bones" in a made-in-Taiwan surveillance system', *ChinAI#214*, online; Sam Biddle, 'US military bought cameras in violation of America's own China sanctions', *The Intercept*, 20 July 2021, online.

122 Kate O'Flaherty, 'All the ways TikTok tracks you and how to stop it', *Wired*, 23 October 2021, online; Sadie Gurman, 'Justice Department probes TikTok's tracking of US journalists', *Wall Street Journal*, 17 March 2023, online.

123 McDade, 'Countries that have banned TikTok as US threatens nationwide ban'; Taylor, 'Australia-wide ban of TikTok on government devices announced as senior politicians quit the app'.

124 Byron Tau, Dustin Volz, 'US state-government websites use TikTok trackers, review finds', *Wall Street Journal*, 21 March 2023, online.

125 'Christopher Wray: 2022 Josh Rosenthal Memorial talk', Policy Talks @ The Ford School, Josh Rosenthal Education Fund Lecture, Ford School, 2 December 2022, online. Testifying to a Senate Intelligence Committee Hearing in March this year, Wray responded in the affirmative to the question 'Could they [the PRC] use it [TikTok] to [control] the software on millions of devices given the opportunity to do so?'; 'FBI Director warns of TikTok security concerns during Senate hearings', *WSJ Video*, 8 March 2023, online.

126 UK Government, *Integrated Review refresh: Responding to a more contested and volatile world*, 50, online.

127 UK Government, *Integrated Review refresh: Responding to a more contested and volatile world*, 33.

128 UK Government, *Integrated Review refresh: Responding to a more contested and volatile world*, 48.

129 Viswanatha et al., 'Pentagon sees giant cargo cranes as possible Chinese spying tools'.

130 'ADIBOT-A Autonomous UV-C Disinfection Robot', UBTECH, online.

131 'PA02 UBTECH Atris', *Rent-A-Robot All-in-one Robotics Marketplace*, online.

132 The Pentagon can approve DJI drones for certain uses provided that they 'are subject to several measures to ensure sensitive data is not released', and the Australian Department of Defence is reviewing their use. Department of Defense, 'Department statement on DJI systems', news release, US Government, 23 July 2021, online; Ellen Whinnett, 'Call for audit as Chinese DJI drones join Australian Defence Force war games', *The Australian*, 16 April 2023, online; Noah Yim, 'DJI drone fleet grounded by Border Force amid links to Chinese military', *The Australian*, 23 May 2023, online.

133 Fergus Hunter, Daria Impiombato, Yvonne Lau , Dr Adam Triggs, Albert Zhang, Urmika Deb, *Countering China's coercive diplomacy*, International Cyber Policy Centre, ASPI, Canberra, 22 February 2023, 1, online.

134 Albee Zhang, Brenda Goh, 'Factbox: Chinese firms working on ChatGPT-style AI technology', *Reuters*, 8 May 2023, online.

135 Qianer Liu, 'China to lay down AI rules with emphasis on content control', *Financial Time*s, 11 July 2023, online.

136 'Can Xi Jinping control AI without crushing it?', *The Economist*, 18 April 2023, online.

137 'Can Xi Jinping control AI without crushing it?'.

138 Justin Bassi, Bec Shrimpton, 'Tech standards setting can't be left to companies or lone nations', *Nikkei Asia*, 9 February 2023, online.

139 'US–EU joint statement of the Trade and Technology Council', The White House, 5 December 2022, online. Eric Schmidt and Yll Bajraktari have gone further to argue that the US should 'integrate its allies in Asia and Europe into a single approach to shaping and promoting democratic digital norms, joint R&D investments, talent exchanges, new regimes for export controls and investment screening, and tech governance issues such as data privacy and content moderation'; Eric Schmidt, Yll Bajraktari, 'America could lose the tech contest with China: how Washington can craft a new strategy', *Foreign Affairs*, 8 September 2022, online.

140 'G7 leaders' statement on economic resilience and economic security'.

141 In February this year, Australia, which takes critical infrastructure protection seriously, updated its Critical Infrastructure Risk Management Program (CIRMP Critical Infrastructure Risk Management Program), Part 2A Security of Critical Infrastructure (SOCI) Act 2018. Cyber and Infrastructure Security Centre, 'Factsheet', Department of Home Affairs, Australian Government, February 2023, online.

Entities responsible for critical infrastructure 'must identify, and as far as is reasonably practicable, take steps to minimise or eliminate … 'material risks' that could have a 'relevant impact' on … the availability, integrity, and reliability of the asset, and the … confidentiality of information about (or within) the asset'. The CIRMP includes obligations to manage the risks we're concerned about here—such as misuse or unauthorised control of a critical infrastructure asset, trusted insiders who have the access and ability to disrupt its functioning, and disruption to critical supply chains by those who purposefully intend to compromise the asset. However, presumably because of the range of hazards responsible entities need to guard against, flexibility is built into how operators address material risks. The intent is that they 'seek to minimise or eliminate material risk where it is reasonably possible' and that governing boards 'should appropriately balance the costs of risk mitigation measures with the impact of those measures in reducing material risk within their own operational context'. Faced with difficult cost/liability/reputational trade-offs across many material risks, it may be difficult for boards to make informed decisions about the level of risk attached to Chinese AI-enabled products and services. Defending against ransomware attacks is self-evidently important because they're common and devastating to a business. By contrast, remote attacks via Chinese vendor equipment might seem like black swan events that can be managed through mitigation, short of going to a more trusted and expensive vendor. In the absence of clear advice and direction from government on the very highest risk categories of Chinese AI-enabled products and services, there's a risk that Australia will end up with a patchwork of different approaches across the program. Hopefully, this will be addressed in the government's forthcoming refreshed cybersecurity strategy.

142 Inglis & Krejsa, 'The cyber social contract: how to rebuild trust in a digital world'.

143 That said, as we become more dependent on AI, cybersecurity will become even more important. Inglis and Krejsa note that emerging AI applications such as autonomous vehicles underline the centrality of a secure cyber-ecosystem. Inglis & Krejsa, 'The cyber social contract: how to rebuild trust in a digital world'. And, of course, the importance of data to AI highlights the need to better protect sovereign data from authoritarian regimes.

144 Ryan et al., *Reining in China's technology giants*, 10.

145 Jack Corrigan, Sergio Fontanez, Michael Kratsios, *Banned in DC: Examining government approaches to foreign technology threats*, Center for Security and Emerging Technology, Georgetown University, October 2022 online.

146 Corrigan et al., *Banned in DC: Examining government approaches to foreign technology threats*.

147 Emily Kilcrease, 'How to win friends and choke China's chip supply', *War on the Rocks*, 6 January 2023, online.

148 Asa Fitch, Yuka Hayashi, John D McKinnon, 'US considers new curbs on AI chip exports to China, *Wall Street Journal*, 27 June 2023, online.

149 ‘Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit’, The White House, 16 September 2022, online.

150 Andrew Duehren, ‘US prepares new rules on investment in China’, *Wall Street Journal*, 3 March 2023, online.

151 ‘Fact sheet: CHIPS and Science Act will lower costs, create jobs, strengthen supply chains, and counter China’, The White House, 9 August 2022, online.

152 ‘Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit’; Chris Inglis, Harry Krejsa, ‘The cyber social contract: how to rebuild trust in a digital world’, *Foreign Affairs*, 21 February 2022, online.

153 ‘Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit’, The White House, 13 July 2021, online; ‘Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit’, The White House, 16 September 2022, online.

154 ‘Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit’.

155 Kilcrease, ‘How to win friends and choke China’s chip supply’.

156 President George W Bush’s Treasury Secretary, Hank Paulson, contests the premise: ‘Washington does not need to encourage deintegration in areas that are not central to national security or the competitiveness of the world’s democracies at the technological bleeding edge’. Henry M Paulson Jr, ‘America’s China policy is not working: the dangers of a broad decoupling, *Foreign Affairs*, 26 January 2023, online.

157 The administration is also seeking to negotiate a ‘Chip 4 alliance’ with Japan, South Korea and Taiwan to coordinate chip policy, although this is complicated by those countries’ high dependence on the China market and competing subsidies among the four. ‘America’s hoped-for Asian semiconductor pact looks tricky’, *The Economist*, 2 February 2023, online.

158 In late January this year, the Biden administration reportedly secured an agreement with the Netherlands and Japan, which are key suppliers of advanced chipmaking equipment, to restrict exports of some machinery to China, and both countries have subsequently taken action. Cagan Koc, Jenny Leonard, ‘Biden wins deal with Netherlands, Japan on China chip export limit’, *Bloomberg*, 28 January 2023, online; Andy Bounds, Qianer Liu, Tim Bradshaw, ‘Dozens of ASML shipments to China face tougher export curbs’, *Financial Times*, 1 July 2023, online.

159 Sarah Bauerle Danzman, Emily Kilcrease, ‘The illusion of controls: unilateral attempts to contain China’s technology ambitions will fail, *Foreign Affairs*, 30 December 2022, online.

160 In late January this year, India’s National Security Adviser, Ajit Doval, led an Indian delegation to Washington for talks with US National Security Advisor Jake Sullivan, Commerce Secretary Gina Raimondo and US industry executives aimed at shifting supply chains in critical technologies, including chips, away from China. Vivian Salama, ‘US pursues India as a supply chain alternative to China’, *Wall Street Journal*, 31 January 2023, online.

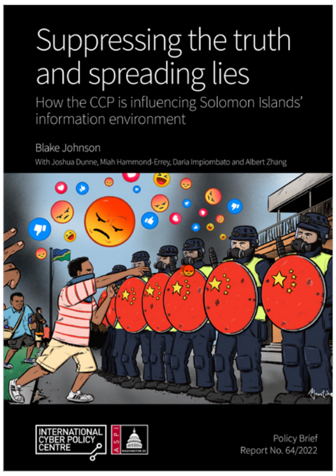
161 As part of a March 2023 restructuring of the bureaucracy, a CCP Central Science and Technology Commission ‘will assume responsibilities for shepherding China’s efforts to develop new capabilities and know-how in strategic sectors’. Chun Han Wong, Keith Zhai, ‘China’s Communist Party overhaul deepens control over finance, technology’, *Wall Street Journal*, 16 March 2023, online. According to State Councillor and Secretary-General of the State Council Xiao Jie, the change will ‘strengthen the centralized and unified leadership of the Chinese Communist Party’s Central Committee over science and technology work’; Evelyn Cheng, ‘China plans to revamp finance, tech oversight’, *CNBC*, 8 March 2023, online.

162 Elliot Ji argues that China’s statist, top-down approach to innovation has impeded progress in China’s semiconductor sector. He notes that China’s ‘Big Fund’ chip investment has been driven by political priorities and therefore focused on the applied and production side (instead of basic science that might lead to innovation and indigenous breakthroughs). Worse than that, ‘the massive injection of capital was done with little institutional oversight … creating incentives for companies and local governments to jump on the bandwagon regardless of their capabilities … leading to rampant corruption and questionable investment decisions such as funding companies with no semiconductor experience to work on chips.’ Elliot Ji, ‘Great Leap Nowhere: the challenges of China’s semiconductor industry’, *War on the Rocks*, 24 February 2023, online. Reinforcing this impression, key officials managing the Big Fund have reportedly been investigated for corruption, along with executives of companies that have received the most funding; Simone Gao, ‘Why China will never lead on tech’, *Wall Street Journal*, 31 January 2023, online.

Acronyms and abbreviations

AGI	artificial general intelligence
AI	artificial intelligence
ASI	artificial superintelligence
CCP	Chinese Communist Party
EU	European Union
GDP	gross domestic product
GPT	generative pre-trained transformer
ICT	information and communications technology
IT	information technology
LLM	large language model
NGO	non-government organisation
NSCAI	National Security Commission on Artificial Intelligence (US)
PRC	People’s Republic of China
RESTRICT Act	Restricting the Emergence of Security Threats That Risk Information and Communications Technology (RESTRICT) Act (US)
STEM	science, technology, engineering and mathematics
TAI	transformative AI
ZPMC	Shanghai Zhenhua Heavy Industries Co. Ltd

Some previous CTS publications



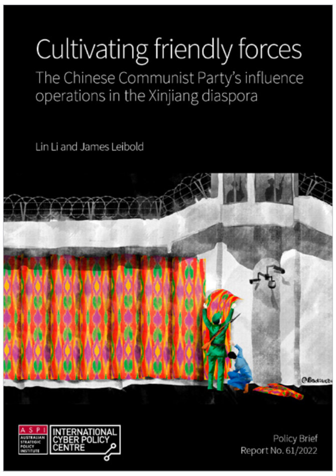
Suppressing the truth and spreading lies

How the CCP is influencing Solomon Islands' information environment

Blake Johnson

With Joshua Dunne, Miah Hammond-Errey, Daria Impiombato and Albert Zhang

Policy Brief
Report No. 64/2022



Cultivating friendly forces

The Chinese Communist Party's influence operations in the Xinjiang diaspora

Lin Li and James Leibold

Policy Brief
Report No. 61/2022

Borrowing mouths to speak on Xinjiang

Fergus Ryan, Ariel Bogle, Nathan Ruser, Albert Zhang and Daria Impiombato

Policy Brief
Report No. 55/2021

Seeking to undermine democracy and partnerships

How the CCP is influencing the Pacific islands information environment

Blake Johnson and Joshua Dunne

Policy Brief
Report No. 70/2023

Assessing the impact of CCP information operations related to Xinjiang

Albert Zhang with Tilla Hoja

Policy Brief
Report No. 62/2022

#StopXinjiang Rumors

The CCP's decentralised disinformation campaign

Fergus Ryan, Ariel Bogle, Albert Zhang and Dr Jacob Wallis

Policy Brief
Report No. 54/2021

Gaming public opinion

The CCP's increasingly sophisticated cyber-enabled influence operations

Albert Zhang

With Tilla Hoja and Jasmine Latimore

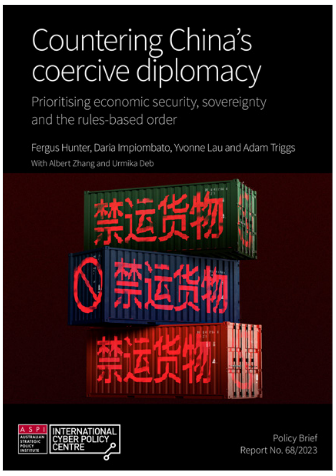
Policy Brief
Report No. 71/2023

China's cyber vision

How the Cyberspace Administration of China is building a new consensus on global internet governance

Dr Nathan Attrill and Audrey Fritz

Policy Brief
Report No. 52/2021



Countering China's coercive diplomacy

Prioritising economic security, sovereignty and the rules-based order

Fergus Hunter, Daria Impiombato, Yvonne Lau and Adam Triggs

With Albert Zhang and Urmika Deb

Policy Brief
Report No. 68/2023

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE