



Council on Geostrategy
CHINA OBSERVATORY

Report
China Observatory
No. 2025/05
February 2025



**COALITION ON
SECURE TECHNOLOGY**

China, science and technology: Advancing geopolitical aims

By Charles Parton

New geostrategic thinking for a more competitive age
<https://www.geostrategy.org.uk>

[THIS PAGE IS INTENTIONALLY LEFT BLANK.]



Contents

Foreword	1
Executive summary	3
1.0 Introduction	7
2.0 Technological changes necessitate greater governmental caution	11
3.0 CCP recognition of the importance of leading science and technology development	12
4.0 Science and technology as the international battleground	14
5.0 A whole-of-state approach to weaponising technology	16
6.0 Weaponising technology: A ‘worst case’ expression	17
7.0 Technology flow to the PRC: The case of a British semiconductor firm	19
8.0 Technology flow from the PRC: The threat of cellular (IoT) modules	21
9.0 Dealing with the threat	24
10. Overarching recommendations	27
10.1 Stemming the outward flow of technology	28
10.2 Protecting against the inward flow dangerous technologies	30
11. Conclusion	32
About the author	33
Acknowledgments	34
About the Council on Geostrategy	35
About the China Observatory	35
Notes	36



Foreword

In recent years, it has become apparent that the People's Republic of China (PRC) is engaged in a struggle with the leading developed countries to dominate science and certain technologies. This is perhaps the most important dimension of 'systemic competition'; Britain's own history shows, perhaps more than any other country, how a small nation can, through scientific and technological mastery, have a decisive impact on international relations, and the development of human society more generally.

The Chinese Communist Party (CCP), is aware of how it can leverage science and technology for geopolitical impact. The problem it has faced is that the PRC has been decades behind the leading Euro-Atlantic powers, as well as Japan and South Korea in the Indo-Pacific. It is determined to catch up. While the CCP has poured resources into research and development, while opening numerous new universities, it has also attempted to seize hold of other countries' scientific and technological know-how through forms of espionage and penetration. Often, the lack of preparedness on the part of the leading democracies has allowed CCP-backed entities to walk straight in.

This Report, by Charles Parton, sets out to answer three interlinked questions: 1. Are the CCP's scientific and technological objectives a threat? 2. What are the dangers of allowing technology to flow to and from the PRC? 3. How can Britain, as well as other free and open countries, mitigate the threat while working with the CCP on other issues where there may be shared interests?

The results are illuminating and should be read and consumed by His Majesty's (HM) Government. For if we are in a period of sustained systemic competition with the PRC, Britain needs to protect its scientific and technological assets, both of which are key to national economic growth and security.

Graeme Downie MP

Chair, Coalition on Secure Technology

James Rogers

Co-founder (Research), Council on Geostrategy



Executive summary

CONTEXT

- Internally, when promulgating to its members the speeches of Xi Jinping, General Secretary of the Chinese Communist Party (CCP), party documents and instructions, the CCP speaks of an ideological struggle between systems in which the People's Republic of China (PRC) will gain domination over the United States (US). Externally, its foreign propaganda system derides the notion of a new cold war, and speaks of 'win-win' or 'a community with a shared future for mankind';
- Xi is clear that dominating the new sciences and technologies is the main means by which the PRC can supplant the US in the world order and change global governance and values;
- The scope of this Report does not include a consideration of the possible effects of the second presidency of Donald Trump, President of the US. However, it is worth noting that a failure to adopt measures to protect the United Kingdom's (UK) science and technology in line with the measures recommended – or variants of them – could lead to severe tensions with the US Government, with adverse effects on trade and other important areas of cooperation, for example under the Five Eyes intelligence sharing alliance;

QUESTIONS THE REPORT ADDRESSES:

- Are the CCP's objectives for science and technology development a threat?
- What are the dangers of allowing technology flow to and from the PRC?
- How can Britain mitigate these threats while maintaining a balance in economic and scientific cooperation?



KEY FINDINGS:

- The CCP is clear that holding key core technologies in its own hands is the only way to guarantee economic and national security. Its ambitions for science and technology development constitute a threat to others. The party applies a ‘whole of state’ approach in using technology to advance its geopolitical aims. It matters not whether a company is state or privately owned, since both must serve CCP aims;
- The governments of free and open countries have yet to adjust to the threat of both the outflow of their technology to the PRC and the inflow of Chinese technology. The latter risks the use of Chinese technology in critical national infrastructure (CNI), which could be disrupted at a time of conflict. The outflow risks British technology being used for military or repressive purposes;
- Three factors have made it difficult for governments of free and open nations to react appropriately to the threat posed by the CCP’s objectives for science and technology:
 1. There is an overestimation of the ‘punishment’ the CCP is able or willing to inflict if foreign countries take measures to protect themselves;
 2. In advising or applying pressure on government, businesses, banks and their lobbyists sometimes place their short-term interests above longer-term and wider national security interests;
 3. Chinese companies, aware of possible legislation coming down the track, are ‘metastasising’ by establishing foreign companies or joint ventures (but in practice whose ultimate ownership and technology are from the PRC) in order to get around future restrictions.

RECOMMENDATIONS:

- Trade, investment, and cooperation on global goods with the PRC should continue, but from a position where security has first been assured. This requires His Majesty’s (HM) Government to:



1. Produce and publish a PRC strategy, outlining a plan for increased research and intelligence in government (from central to regional) on the capabilities and direction of Chinese science and technology, and the ways they pose a threat, while also providing an outline for balanced engagement in other areas;
 2. Officially recognise within the government that the PRC is a threat and that more thorough implementation – and possibly amendment – of existing security and procurement laws is needed;
 3. Establish a government scientific advisory board to advise on the appropriateness of technological collaboration or investment with the PRC. It would work closely with the existing, but reinforced, Research Collaboration Advisory Team. It would also advise on areas of technology where the concept of ‘trusted suppliers’ should be enforced;
 4. Establish a coordinating body to oversee planning and implementation of protective measures across government. Currently, no such body has sufficient focus. The remits of the Joint State Threats Assessment Team (JSTAT) and the National Cyber Security Centre (NCSC) do not cover the waterfront of the science and technology threat;
 5. Better resource the Investment Security Unit to ensure more thorough implementation of the National Security Investment Act (NSIA), including mandatory reporting for all cases involving the PRC, and improved government market monitoring. Strengthen other defences, such as the Academic Technology Approval Scheme and rigorous use of the ‘debarment list’ under the Procurement Act, in order to keep out Chinese technology which is a threat to national security;
 6. Place the PRC on the ‘enhanced tier’ of the Foreign Interests Registration Scheme (FIRS) under the National Security Act, thereby requiring UK entities working with the PRC to declare such work;
-



7. Strengthen the powers of the Advisory Committee on Business Appointments (ACOBA), to ensure that after retirement, ministers and senior officials do not prejudice national interests by inappropriate use of information gained from their time in government. This would also help to ensure that while still in office, the decision making of ministers and officials would not be influenced by the effects on possible future job offers;
8. Reduce the need for hi-technology startups to sell themselves to Chinese entities by boosting the National Strategic Security Investment Fund, HM Government's corporate venturing arm for dual-use advanced technologies. The government should take a golden share in at risk companies.

1.0 Introduction

Clarity on the question of whether the People's Republic of China (PRC) is a threat is vital.¹ Firstly, the obvious needs restating: 'China' means the Chinese Communist Party (CCP). As Xi Jinping, General Secretary of the CCP, likes to say, 'South, north, east and west, the communist party leads everything.'²

Secondly, the current world order is under threat – the system of global governance, laws and values established after the Second World War by the victors. Western powers were buttressed by the institutions and norms established. The CCP wishes to change current global governance and is prepared to fight hard and outside the hitherto accepted rules of competition.

The CCP puts out two types of narrative. The first it terms 'foreign propaganda' [外宣], the language of 'win-win', 'community of shared destiny for mankind', and the Global Development, Global Security, and Global Civilisation initiatives. The second narrative is what it puts out to party members for guidance and reassurance. It is this which better represents its true intentions and therefore to which foreign governments should pay attention.

The CCP declares its 'Second Centennial Goal' as being, by 2049, to establish a PRC which is a 'modern socialist country that is prosperous, strong, democratic, culturally advanced and harmonious'. Behind this reassuring language lies a more muscular intention: to ensure that the PRC replaces the United States (US) as the leading superpower, and to reorder global governance better to suit CCP interests and values.

To achieve that, the CCP under Xi sees itself engaged in a fierce 'struggle' against 'hostile foreign forces'. For all its accusations that 'certain countries' are guilty of a 'cold war mentality', the CCP itself is in no doubt that this is a cold war – and an ideological one.³ As Xi has said, 'competition between systems is an important aspect of competition for comprehensive national power', and the dominance of a system gives a country the dominant position in winning the 'strategic initiative' – a

¹ For a longer discussion of the CCP as a threat, see: Charles Parton, 'Is China a threat?', Council on Geostrategy, 16/03/2023, <https://www.geostrategy.org.uk/> (checked: 24/02/2025).

² Weiyi Cai, Aaron Byrd, Chris Buck, 'How Xi Returned China to One-Man Rule', *New York Times*, 02/09/2023, <https://www.nytimes.com/> (checked: 24/02/2025).

³ For a balanced and sobering examination of the nature of the new cold war and of its ideological nature, see: Robin Niblett, *The New Cold War* (London: Atlantic Books, 2024).



stronger term than the English translation suggests.⁴ CCP documents, speeches and Central Committee commentaries in party media (all important in promulgating the party centre's views and instructions) make clear that the cornerstone of CCP foreign policy is deep hostility and suspicion to the US; that this extends to the question of values; and that under the name of Chinese modernisation the ideological battlefield is located in the so-called 'Global South'.

Ultimately, the CCP believes it should win this war without military confrontation – even if the threat of military action is part of the armoury.

Box 1: The CCP leadership's views on the struggle with the US and its allies

- 'We must diligently prepare for a long period of cooperation and of conflict between these two social systems in each of these domains (economic, technological, and military);'⁵
- '...the position of Western anti-China forces to pressure for urgent reform won't change, and they will continue to point the spearhead of Westernising, splitting, and "Colour Revolutions" at China';⁶
- 'International struggles are becoming increasingly fierce, and system confrontation has become a prominent feature of the game between major powers. The US suppression [of us] is a major threat but [our struggle with the US] is both a skirmish and a protracted war;'⁷

⁴ See: 张晓松 [Zhang Xiaosong] et al., '继续奋斗，走好新时代赶考路' ['Continue to struggle, and take the testing road in the new era'], 人民日报 [People's Daily], 08/11/2021, <http://www.people.com.cn/> (checked: 24/02/2025).

⁵ Xi's first address to the Central Committee in January 2013, see: Tanner Greer, 'Xi Jinping in Translation: China's Guiding Ideology', *Palladium Magazine*, 31/05/2019, <https://www.palladiummag.com/> (checked: 24/02/2025).

⁶ *Ibid.*

⁷ Chen Yixin, 'The time for China's rise has come, security chief tells law enforcers', *South China Morning Post*, 15/01/2021, <https://www.scmp.com/> (checked: 24/02/2025).



- ‘Various hostile forces will never allow us to realise the great rejuvenation of the Chinese nation smoothly’;⁸
- The struggle between two social systems and two ideologies will also be long-term, complex, arduous and severe. The strategic contest between China and the United States is bound to last for a long period of time, for which we must be fully prepared ideologically and work;⁹
- Hostile forces persistently seek to ferment [sic] a ‘Colour Revolution’ within our state, vainly attempting to subvert the leadership of the Chinese Communist Party and the socialist institutions of our state...On the international stage, Western hostile forces have not ceased their ideological infiltration of our country, not even for a moment. They do everything in their power to promote so-called ‘universal values’.¹⁰
- We must be highly vigilant against external forces fomenting a ‘new cold war’ and creating confrontation in the region, and resolutely oppose any country interfering in internal affairs and staging a ‘colour revolution’ for any reason.¹¹

On the export of ideology, Xi has made explicit that ‘Chinese modernisation’, defined in terms of the CCP’s systems and values,

⁸ 习近平 [Xi Jinping], Speech: ‘以史为鉴、开创未来 埋头苦干、勇毅前行’ [‘Take history as a mirror, create the future, work hard, and move forward bravely’], 求是 [Qiushi], 01/01/2022, <http://www.qstheory.cn/> (checked: 24/02/2025).

⁹ These words are from 曲青山 [Qu Qingshan], Director of the Central Party History and Literature Research Institute, an important ideological organisation within the party. For further details, see: ‘新征程 新思想 新篇章 | 从未来维度认识把握“两个确立”’ [‘New Journey, New Thought, New Chapter, Understanding and Grasping the “Two Establishments” from the Future Dimension’], 中国共产党中央纪律检查委员会 [Central Commission for Discipline Inspection and National Supervisory Commission of the People’s Republic of China], 07/07/2022, <https://www.ccdi.gov.cn/> (checked: 24/02/2025).

¹⁰ It is worth noting that these ‘universal values’ were laid down in the 1948 Universal Declaration of Human Rights and that two Chinese scholars played instrumental roles in the UN Commission. See: ‘总体国家安全观学习纲要’ [‘The Total National Security Paradigm: A Study Outline’], 中央国家安全委员会办公室 [Office of the Central National Security Commission], trans. Kitsch Liao, 01/01/2023, <https://www.strategictranslation.org/> (checked: 24/02/2025).

¹¹ ‘China’s President Xi Jinping warns against “New Cold War” at SCO summit’, *Firstpost*, 04/07/2023, <https://www.firstpost.com/> (checked: 24/02/2025).



is a model for developing countries to adopt in place of the modernisation concepts of the free and open countries which have failed to help emerging nations.

- Chinese-style modernisation...provides a brand-new model of modernisation for the whole world...it transcends the theory and practice of Western-style modernisation...and provides a brand-new choice for the vast number of developing countries.¹²

The CCP employs a variety of strategies in its aim to supersede the US as the pre-eminent global superpower, via the ‘Second Centennial Goal’. Three relate to science and technology:

1. **Data.** ‘Data is the new oil’ – there is a reason for clichés. The CCP has set about collecting, and further developing the capability of collecting, vast amounts of data, both legitimately and illegitimately (its efforts devoted to cyber attacks are enormous);
2. **Dominating the new sciences and technologies.** This prioritises dominating new industries growing from the data driven technological revolution. Internally, policies of subsidy, but also cut-throat competition between Chinese industries, have made them highly effective; externally, acquisition, commissioning research, espionage, hacking and other dubious practices have put the PRC in a strong position;
3. **Creating dependencies.** CCP policies have not just given the PRC the ability to use dependencies on minerals such as rare earths, but to exploit dependencies on telecoms (Huawei), cellular Internet of Things (IoT) modules (Quectel), batteries and more.

¹² This is from Xi’s address to the Central Party School in February 2023. See: ‘话讲要重表发上式班开班讨论研精大十二的党彻贯习学在平近习’ [‘Xi Jinping delivered an important speech at the opening ceremony of the seminar on studying and implementing the spirit of the 20th National Congress of the Communist Party of China’], 新华社 [Xinhua], 07/02/2023, <https://www.gov.cn/> (checked: 24/02/2025).



2.0 Technological changes necessitate greater governmental caution

The new government of the United Kingdom (UK) has rightly emphasised that its first priority is security.¹³ The prime duty of any government is to protect critical national infrastructure (CNI). The distinction between economic security and national security is shrinking.

The duty of the state to make its CNI proof against its enemies is now more onerous, and not just because of the ‘high winds, choppy waters, and even dangerous storms of global turbulence’.¹⁴ The definition of what constitutes CNI has broadened from traditional areas such as power generation and transmission, transport, food infrastructure, energy and water supplies, and telecommunications. The advent of the Internet of Things (IoT) means that modern cars (now in essence computers/smartphones on wheels) and their charging points, smart meters, financial and payment systems, and many other areas could be used to disrupt or destroy on a scale as great as a direct attack on a power station or water supply system.

A third age is dawning in which the Internet of Things (IoT), Artificial Intelligence (AI) and quantum computing will further increase these challenges.

¹³ David Lammy, ‘Britain Reconnected: A Foreign Policy for Security and Prosperity at Home’, Fabian Society, 28/03/2023, <https://fabians.org.uk/> (checked: 24/02/2025).

¹⁴ Yang Sheng et al., ‘How will CPC withstand ‘dangerous storms’ in the future?’, *Global Times*, 17/10/2022, <https://www.globaltimes.cn/> (checked: 24/02/2025).

3.0 CCP recognition of the importance of leading science and technology development

The CCP has long decided that the PRC must rely on its own scientific and technological resources rather than on those of liberal democracies and must establish itself as a global leader. In 2003, it began work on a 'Medium- and Long-term Plan for S&T Development', which was published in 2006.¹⁵ That plan and subsequent plans, such as the 2014 'National Semi-conductor Plan', the 2015 'Made in China 2025' industrial policy and the 2016 'S&T Innovation 2030 Project', are woven into the fabric of the party's 'Five Year Plans' to ensure implementation.¹⁶

At the First Session of the 14th National People's Congress (NPC) in 2023, Xi announced a reorganisation of the PRC's science and technology administration. A new Central Commission on Science and Technology emerged. Although information about its workings – and indeed number of meetings – has been sparse, it is clearly an attempt to focus resources better on the aim of leading global science and technology, with a strong eye on the geopolitical implications. Influential commentaries and articles in party media at the time of the First Session of the 14th NPC in 2023 made that point clearly:

To a certain extent, those who gain access to the internet will gain the world. Seizing the historical opportunity of the information revolution is a major strategic decision related to the construction of a strong country and national rejuvenation. Core technology is an important weapon for the country....Only by holding key core technologies in our own hands can we fundamentally guarantee

¹⁵ Yuxuan Jia and Andy Han, 'BGI's Mei Yonghong on China's past, present, & future in science & technology', *The East is Read*, 21/12/2024, <https://www.eastisread.com/> (checked: 24/02/2025). For details of the Medium-and Long-term Plan for S&T Development, see: '国家中长期科学和技术发展规划纲要' ['Outline of the National Medium- and Long-Term Science and Technology Development Plan'], 中华人民共和国国务院 [State Council of the People's Republic of China], 09/02/2006, <https://www.gov.cn/> (checked: 24/02/2025).

¹⁶ For an account of these plans, see: Karen Sutter, 'Foreign Technology Transfer Through Commerce', William C. Hannas and Didi Kirsten Tatlow (ed.), *China's quest for foreign technology*, (London: Routledge, 2020).



national economic security, national defence security, and other security.¹⁷

¹⁷ 信平 [Xin Ping], ‘这十年, 我们阔步迈向网络强国’ [‘In the past decade, we have made great strides towards becoming a cyber power’], 人民日报 [People’s Daily], 19/03/2024, <http://paper.people.com.cn/> (checked: 24/02/2025).



4.0 Science and technology as the international battleground

As the US has continued to take measures to slow the progress of Chinese technological development, so Xi and party leaders have become ever more urgent in their emphasis on becoming a global science power and outstripping the Americans. In June 2024, the CCP held a science and technology conference. In his speech, Xi declared that high-technology fields had become the forefront and main battleground of international competition, profoundly reshaping the global order and the development landscape. Among five major points, the third was a call for ‘strong international influence and leadership’. The reason, he stressed, for improving science and technology planning and for strengthening the coordination of efforts between the central and local governments was ‘to build highlands for innovation with global influence’.¹⁸

Following any conference and speech by Xi, the party is then enjoined to study the results. The second half of 2024 thus saw a sharpening of the emphasis on science and technology as a, if not the, major means to achieve national power. A common theme of articles amplifying Xi’s message on technology is that in the struggle with the US (unstated, but mentioned as ‘competition for national strength’) what is crucial is the competition over science and technology and ultimately ‘the underlying contest is whose system is superior’.¹⁹ As the minister of science and technology writing in the *People’s Daily*, the CCP’s newspaper, bluntly put it in August:

...the scientific and technological revolution and the contest between major powers are intertwined; the high-tech field has become the forefront and main battlefield of international competition, profoundly influencing the global order and development pattern...the competition between countries is a competition of strength. What is crucial is the competition of

¹⁸ ‘Full text of Xi’s speech at sci-tech conference’, ECNS, 28/06/2024, <http://www.ecns.cn/> (checked: 24/02/2025).

¹⁹ This is a translation of a line in a speech by Xi: [‘国家实力之争关键是科技创新能力之争，背后较量的是谁的制度更优越。’]. See: 阴和俊 [Yin Hejun], ‘深化科技体制改革’ [‘Deepen the reform of the science and technology system’], 人民日报 [People’s Daily], 22/08/2024, <http://paper.people.com.cn/> (checked: 24/02/2025).



scientific and technological innovation capabilities. The underlying contest is about whose system is superior.²⁰

A month later the same message using the same language was hammered home by the CCP's Theoretical Learning Centre Group of the Ministry of Science and Technology, in *Qiushi*, the CCP's theoretical journal.²¹

It is a view shared by Chinese businesses. In a recent speech by Mei Hongyong, Director of the BGI Group, one of the PRC's leading technology companies, and formerly an official at the Ministry of Science and Technology, said:

The core of the US-China rivalry is the technology war...Many people talk about financial and trade wars, but the deadliest battle is the technology war. The technology war will ultimately determine the fate of both sides. Whether the US can defeat China or whether China can rise from adversity will depend on the technology war. I also believe that the technology war is not an encounter battle, but protracted.²²

The noted scholar of international relations Yan Xuetong, a Professor at Tsinghua University, has also been clear that competition between the US and the PRC is intense, and although a proxy war is unlikely, 'in the digital age, the outcome of US-PRC competition will be determined by technological superiority.'²³

No one should doubt that Xi and the CCP see science and technology as the main tool, if not weapon, in the struggle between nations.

²⁰ 阴和俊 [Yin Hejun], '深化科技体制改革 (学习贯彻党的二十届三中全会精神)' ['Deepen the reform of the science and technology system (study and implement the spirit of the Third Plenary Session of the 20th CPC Central Committee)'], 人民日报 [People's Daily], 22/08/2024, <http://paper.people.com.cn/> (checked: 24/02/2025).

²¹ 'Deepen the reform of the science and technology system and provide strong scientific and technological support for China's modernisation', (深化科技体制改革 为中国式现代化提供强大科技支撑), 求是 [Qiushi], 16/09/2024, <http://www.qstheory.cn/> (checked: 24/02/2025).

²² Yuxuan Jia and Andy Han, 'BGI's Mei Yonghong on China's past, present, & future in science & technology', *The East is Read*, 21/12/2024, <https://www.eastisread.com/> (checked: 24/02/2025).

²³ Yuxuan Jia and Shuyang Yu, 'Yan Xuetong predicts Trump & China-US competition', *The East is Read*, 24/01/2025, <https://www.eastisread.com/> (checked: 24/02/2025).



5.0 A whole-of-state approach to weaponising technology

Bringing intentions into reality is never easy for governments. However, the CCP's Leninist system allows a more effective implementation. The party requires and ensures a whole of state approach of technology as a vital component of security. Chinese companies and Chinese individuals have no choice but to obey the diktats of the CCP. National security laws ordain that both organisations and individuals must accede to the requests of the security authorities. What constitutes a security matter is left deliberately vague by the laws. Refusal to cooperate in what the party decides to define as a security issue would be highly dangerous.

Yet, irrespective of security considerations or laws, no company management, state owned or private, could turn down a CCP instruction. No matter their ownership structure, all companies must function as tools of the party when requested. Indeed, the party cells and branches established within them would ensure compliance (by 2017, 92% of the top 500 firms and 73% of all private companies had embedded party organisations.²⁴ Xi has since ensured that the figure is higher). Furthermore, most individuals in positions of authority within a company or organisation will be party members. That too means obeying CCP directives or facing disciplinary action.

There are other incentives for Chinese companies, organisations and individuals to help the party's use of science and technology as a geopolitical weapon. In addition to feelings of patriotism, they benefit from state support for champions in the new technologies and industries. The CCP ensures that companies receive favourable regulatory treatment, finance at preferential rates through central and regional banking institutions, access to key materials and products (such as semiconductors) at below cost, shared research and other state support.

²⁴ Jerome Doyon, 'CCP branches out into private businesses', East Asia Forum, 11/08/2023, <https://eastasiaforum.org> (checked: 24/02/2025).



6.0 Weaponising technology: A 'worst case' expression

It is the basic duty of the government to defend the nation against the possibility of worse cases. David Lammy, Foreign Secretary, rightly declared that 'We will prioritise Britain's national security above all else.'²⁵ The CCP is clear that holding key core technologies in its own hands is the only way to guarantee economic and national security. His Majesty's (HM) Government should be equally clear. This is far more serious than just a question of commercial advantage.

The long-term threats to Britain's national security are threefold:

1. **Dependencies.** Dependencies relating to new technologies and industries, components and systems, are every bit as dangerous as dependencies on minerals, materials and resources, such as rare earths, lithium, or gallium. Dependencies on such materials would allow the CCP to demand of other governments that they change their policies – and not just in the area of economic and commercial relations – or else face the threat of economic harm or worse;
2. **Disruption and even destruction.** Domination, and, worse, monopoly of certain new technologies and industries would give the CCP the power to degrade or turn off other countries' economies (if nothing else, the Israeli use of paggers to assassinate members of Hamas showed the power of remote access). In normal times, the CCP will not pursue its geopolitical aims by disruption or destruction. That would destroy its markets. But history is littered with wars. The CCP is preparing to win without fighting. Free and open countries are failing their future generations if they do not prepare their defences;
3. **Data.** The CCP collects foreign data on an epic scale. It has a deep understanding of the weaknesses of use, transmission and storage, which is why it aims to control not just the systems which generate data, but also those which transmit and store it. The threat is becoming more acute with the advent of machine learning,

²⁵ David Lammy, 'Britain Reconnected: A Foreign Policy for Security and Prosperity at Home', Fabian Society, 28/03/2023, <https://fabians.org.uk/> (checked: 24/02/2025).



artificial intelligence and eventually quantum computing. It ranges from the power of aggregated data to the ability to build detailed patterns of life pictures of individuals, including of senior officials or those in sensitive jobs, who might be targeted for intelligence approaches or disruption.

The threat from an unregulated flow of technology works in both directions – to the PRC and from the PRC. The next part of this paper looks at an example of each.



7.0 Technology flow to the PRC: The case of a British semiconductor firm

This section draws on the important paper put out by UK Transparency International (UKCT).²⁶ The paper should be required reading for those charged with defending the UK's economic and national security as it epitomises regulatory failure rather than the pursuit of national interest.

The aforementioned paper uses as an example a British microchip design company specialising in graphics processing unit (GPU) design, which is vital for the development of chips used in advanced Artificial Intelligence (AI). The technology is used in many areas, but is important for military and missile applications. In 2017, UKCT says that a Chinese-owned fund bought the company. What is unusual about this fund – originally registered in Delaware in the US – is that it is reported to have only one funder and to have invested in only one other small company besides the British microchip company in question. This is not the norm when it comes to funds spreading financial risk. According to UKCT, the funder is a Chinese state-owned company whose annual report stated that the company aimed to 'invest in strategic emerging industries related to national security'. The UKCT report uses Chinese company data to show the funder (the Chinese state-owned company) has invested in military companies.

Despite the US Government refusing to allow the Chinese-owned fund to take over a technology company on national security grounds, HM Government permitted its takeover of this British microchip company. Assurances were given that the funder – the Chinese state-owned company – did not control the Chinese-owned fund, and that it would not move the head office and operations to the PRC.

Yet, in 2020, according to company insiders, a plan was put into operation to transfer core assets of the British microchip company to the PRC; importantly, this included having British experts hand over the 'know how' (intellectual property cannot be properly exploited without

²⁶ 'Imagination Technologies and Asset Stripping by the Chinese Communist Party – Part One', UK-China Transparency, 03/12/2024, <https://ukctransparency.org/> (checked: 24/02/2025). See also: Tom Burgis, 'Chinese AI chip firms blacklisted over weapons concerns gained access to UK technology', *The Guardian*, 18/12/2024, <https://www.theguardian.com/> (checked: 24/02/2025).



training and the transfer of years of accumulated experience).²⁷ Such a transfer would allow the recipients to dispense with the British microchip company in the future. UKCT reports that the recipients were three companies with extensive links to the CCP's military; two are subject to American sanctions.

While this case occurred before the National Security Investment Act (NSIA) came into force in January 2022, it shows how, even with a governmental review taking place, national decision making was inadequate. HM Government can also apply a retrospective use of the call-in power under the Act, but has so far not chosen to do so. Indeed, a very senior member of government told the author that there was a case 'far worse' than this British microchip company, in which the UK had 'helped to advance Chinese military capability by years'.²⁸

²⁷ 'Imagination Technologies and Asset Stripping by the Chinese Communist Party – Part One', UK-China Transparency, 03/12/2024, <https://ukctransparency.org/>, (checked: 24/02/2025).

²⁸ The source did not vouch for details because of the sensitivity of the case.



8.0 Technology flow from the PRC: The threat of cellular (IoT) modules

Cellular IoT modules (CIMs) are small components embedded within equipment or devices. They include software processing, geolocation capability, e-sims and other peripheral components. They connect to the internet, transmit, receive and process vast amounts of data about their environments, independent of human action (IoT). They monitor and control complex systems remotely. The potential risks of this have been outlined extensively.²⁹ To ensure that such systems run efficiently, they collect huge amounts of data and metadata for analysis, processing, and response management. They also deliver software and firmware updates to improve functionality. They are, in effect, the gateway to computers and systems. CIMs are essential to a modern economy and life. It is estimated that there will be over 6.2 billion CIM connections by 2030.³⁰

The CCP is fully aware of the strategic importance of the CIM industry. Through companies such as Quectel, Fibocom, MeiG and others it aims to achieve a Chinese monopoly. Efficient though these companies are, they also benefit from the usual subsidies, cheap financing or land and other state given advantages, as they seek to drive non-Chinese competitors into oblivion (two such, Ublox and Sierra Wireless, are currently looking for buyers). Chinese companies had over 70% of the global market at the end of 2023.³¹

If achieved in future, a monopoly of the supply of CIMs would enable the CCP to use the three threats of dependency, disruption and data (as set out above). It is worth setting out a few examples of threats which could be operationalised, such as:

- Destroying the power grid through high voltage attacks, for example, by remote programming so that during very hot weather

²⁹ See (in order of length): Charles Parton, 'The Infrastructure Threat from Chinese Cellular (IoT) Modules (CIMs)', Coalition on Secure Technology, 10/10/2024, <https://cim-coalition.co.uk/> (checked: 24/02/2025). Charles Parton, 'Chinese cellular (IoT) modules: Countering the threat', Council on Geostrategy, 19/03/2024, <https://www.geostrategy.org.uk/> (checked: 24/02/2025). Charles Parton, 'Cellular IoT modules – Supply Chain Security', Oodaloop, 23/01/2023, <https://oodaloop.com/> (checked: 24/02/2025).

³⁰ 'Global Cellular IoT Connectivity Revenue to Exceed \$26 Billion by 2030', Counterpoint Research, 19/09/2024, <https://www.counterpointresearch.com/> (checked: 24/02/2025).

³¹ *Ibid.*



all air-conditioners, washing machines and other white goods switch on to full power simultaneously, combined with malware to ensure that smart meters misbehave. This could unbalance the grid sufficiently to blow large transformers. Meanwhile, the Chinese have been scoping out American critical national infrastructure in an attack dubbed VOLT TYPHOON.³²

- Switching off cranes at ports, for example, to prevent arms being loaded and sent to the western Pacific. This is what lies behind recent American concerns about ZPMC cranes, which have Quectel CIMs.³³
- Interfering with food security and production by remotely switching off agricultural machinery. This is what John Deere did to machinery stolen by the Russians from Ukraine.³⁴ But this power is not limited to the machinery manufacturers and operators: CIM suppliers could send in malware via their regular firmware updates and achieve the same result.
- Building ‘pattern of life’ pictures of individuals, including of senior officials and those in sensitive jobs. In late 2022, the UK security authorities stripped down the Prime Minister’s car because ‘data was emanating through the “e-sim” – that is the CIM – to China’.³⁵ Synching a smart phone to a car’s audio system would allow the exfiltration of large amounts of the data on the phone through the CIM. The vulnerability of vehicles is shown by the Tesla engineers, who were sacked for remotely looking at video and images taken from in private individuals’ cars.³⁶
- Accessing data and metadata from telecoms systems. While many governments have banned Huawei from their phone networks, vulnerabilities remain because Chinese CIMs are present in many models of routers.
- Bringing transport to a halt, whether by disrupting traffic controls or by using access via the CIM to disable lorries – how, for example,

³² Arielle Waldman, ‘CISA: Volt Typhoon had access to some US targets for 5 years’, TechTarget, 07/02/2024, <https://www.techtarget.com/> (checked: 24/02/2025).

³³ Carter Evans, Paul Facey, ‘Chinese cranes at U.S. ports raise homeland security concerns’, CBS News, 11/02/2025, <https://www.cbsnews.com/> (checked: 24/02/2025).

³⁴ Emma Roth, ‘Remote lockouts reportedly stop Russian troops from using stolen Ukrainian farm equipment’, The Verge, 02/05/2022, <https://www.theverge.com/> (checked: 24/02/2025).

³⁵ That the car was the prime minister’s was confirmed by two well placed sources. For example, see: Richard Holmes, ‘Hidden Chinese tracking device ‘found in UK Government car’ sparks national security fears’, The i Paper, 06/01/2023, <https://inews.co.uk/> (checked: 24/02/2025).

³⁶ Steve Stecklow et al., ‘Tesla workers shared sensitive images recorded by customer cars’, Reuters, 06/04/2023, <https://www.reuters.com/> (checked: 24/02/2025).



would India then be able to move men and materiel up to the Tibetan border if hostilities broke out?

9.0 Dealing with the threat

There are benefits from collaboration with the PRC in science and technology – economic, environmental and innovation from in scientific cooperation. Academia has genuine concerns about potential losses from a move away from traditional openness in scientific cooperation. The CCP is solipsistic, but governments should at least try to convince it that observing internationally-agreed rules brings advantages.

Nevertheless, HM Government needs to recognise that no other authoritarian regime plays an equivalent role in academic and research cooperation or in hi-technology trade and investment such as the PRC. Xi and his party already consider themselves to be in a technology war. Yet by continuing to dither, free and open countries only increase inevitable long-term costs.

The first priority is therefore to ensure economic and national security, to rule out clearly unacceptable areas of cooperation or partners – just as the CCP does – and then, strictly observing those limitations, maximise cooperation in unthreatening domains.

Several factors make it harder for governments to protect their nations' interests. In particular, there is exaggerated fear from governments that the CCP will threaten exports and investment. Ministerial visits may be curtailed, but exports of all countries which have been put in the 'diplomatic doghouse' have risen.³⁷ For the UK, exports rose during the period of frozen relations after the prime minister met the Dalai Lama. They fell in 2015 after the announcement of the 'Golden era'. Despite measures introduced by the Conservative government to protect the UK against Chinese interference, in 2022, exports reached a record US\$35.6 billion (£28.2 billion) and a slightly lower US\$34.3 billion (£27.2 billion) in 2023.

Governments should also be careful to avoid thinking that Chinese investment is a charity with big pockets. In the case of Britain, in 2022, the PRC accounted for 0.2% of the total UK inward Foreign Direct Investment (FDI) stock.³⁸ Since 2016, the CCP has increased oversight of Chinese investment, to ensure that it meets CCP objectives, largely related to acquiring technology to fill the gaps which its 'dual circulation' policy

³⁷ For further details, see: Charles Parton, 'Empty threats? Policy making amidst Chinese pressure', Council on Geostrategy, 06/07/2021, <https://www.geostrategy.org.uk/> (checked: 24/02/2025).

³⁸ 'Trade and Investment Factsheet – China', Department for Business and Trade (UK), 31/01/2025, <https://www.gov.uk/> (checked: 24/02/2025).

has identified. In many cases, countries should not be handing over such technologies.

In general, there are four reasons for welcoming investment, none of which are cogent in the case of the UK and the PRC:

1. **To create jobs.** Yet the contribution of Chinese investment has been small; for example, around 9,400 jobs created and maintained within the three years 2016–2017 to 2018–2019.³⁹ The case of the British microchip company does not reassure: average staffing dropped from 1,100 in 2016 to 520 in 2023. It is not clear how many of those losses are in the UK (presumably the majority), but in late 2023, the company intended to lay off 20% of its British staff.
2. **To obtain new technology.** But the flow is to the PRC, not from the PRC.
3. **To learn new management techniques.** Again, the flow has been to the PRC.
4. **To obtain capital to promote the business.** Here, HM Government should decide in which areas economic and national security concerns must trump investment from the PRC; for example, whether some form of industrial policy is needed to ensure the survival of key industries for the future. The case of new energy vehicles is a salient one: too little consideration has been given to the security implications, via the CIMs in particular.

Protecting the economic and national security of free and open countries is made harder by the role played by their businesses, banks and their lobbyists, who often put their short-term interests above longer-term and wider national security concerns. When asked why they were not raising the issue of unfair competition, the response of an executive of a CIM manufacturing company was that the owners, an investment fund, did not wish to ‘rock the boat’ – presumably because their main aim is to sell the company.⁴⁰ In another instance, in the US, an amendment to the 2024 National Defence Authorisation Act (NDAA) put up by Raja Krishnamoorthi (Democratic Party) Chairman of the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, was unexpectedly opposed by the Republican side after objections from a senator and house representatives from Ohio, a state

³⁹ Matthew Haynes et al., ‘UK jobs dependent on links to China’, China-Britain Business Council, 14/07/2020, <https://www.cbbc.org/> (checked: 24/02/2025).

⁴⁰ Author’s private conversation in 2023.



with hitherto no indigenous CIM interests.⁴¹ Subsequently Quectel, the Chinese CIM manufacturer, announced a US\$14 million investment in Ohio through Eagle Electronics.⁴² Two other large American companies, which work closely with Quectel and have significant profits derived from the PRC, are thought to be behind the lobbying which led to the withdrawal of the NDAA amendment.⁴³

A further problem is that Chinese companies, aware of possible legislation coming down the track, are ‘metastasising’ by establishing foreign companies or joint ventures. Thus, in the CIM field, Quectel has set up Ikotek (for design) and Netprisma (for manufacture, in Malaysia), representing them as legally American. Declaring that these companies are ‘American’ does not diminish the threat they pose. In the words of a CIM engineer:

It is still 100% a Quectel piece of hardware and software wrapped in a US flag. It is...licensed and built in the US...The firmware inside the module is still designed and supported by Quectel.⁴⁴

⁴¹ ‘Amendment to Rules Committee, Print 118–36, Offered by Mr. Krishnamoorthi of Illinois’, House of Representatives (US), 11/06/2024, <https://www.house.gov/> (checked: 24/02/2025).

⁴² ‘Eagle Electronics Announces Formation of State-of-the-Art Electronics Manufacturing Facility, \$14mm of Funding, and Customer Commitments’, *PR Newswire*, 03/12/2024, <https://www.prnewswire.com/> (checked: 24/02/2025).

⁴³ Given the propensity of companies to launch lawsuits aimed at silencing the less financially endowed, the author will not name them.

⁴⁴ To the author in a private communication.



10. Overarching recommendations

Dealing with the threat requires:

- **Produce and publish a PRC strategy.** A strategy would define the balance between security and economic benefit in the context of the PRC. Despite calls in parliament and elsewhere the previous Conservative government conspicuously failed in this task; the current Labour government has delayed its 'China audit' and is ambiguous on its intentions for a strategy.
- **Increase intelligence and research on the capabilities and direction of Chinese science and technology.** This is a task not just for the intelligence services, but also for open source intelligence, whether through HM Government's own capabilities or by buying in more services than at present.
- **Recognise officially within government that the PRC is a threat** and that countering that threat requires special measures. Legislation such as the National Security Investment Act (NSIA), National Security Act, the Procurement Act should be applied in ways to reflect this status, or, if necessary, should be amended.
- **Raise awareness within government, including regional governments, of the level and nature of the threat from Chinese science and technology.** For example, the understanding within government of the threat of CIMs to economic and national security is limited. The government should be on top of the moves of Chinese companies aimed at vitiating protective measures, such as setting up alternate companies which are ostensibly not Chinese.
- **Update continually the redefinition of what constitutes CNI** in the light of developments in science and technology, and given greater visibility of CCP intentions. This should be promulgated throughout government departments.
- **Establish a coordinating body, a centre of expertise on science and technology security,** to oversee planning and implementation of protective measures across government. Currently, no such body has sufficient focus. The Joint State Threats Assessment Team (JSTAT) was set up in 2017 and only openly acknowledged in 2020.⁴⁵

⁴⁵ 'Counter State Based Threats', Parliament (UK), 17/03/2020, <https://questions-statements.parliament.uk/> (checked: 24/02/2025).



The Security Service's website refers to it as countering 'activities such as espionage, assassination, and interference in our democracy, and threats to the UK's economic security'.⁴⁶ It is not focussed specifically on the science and technology threat, and few in government departments are aware of it. Likewise, the National Cyber Security Centre (NCSC) has the narrow remit of being the UK's technical authority for cyber security, but does not oversee the wider threat.

- **Keep in step with allies and partners.** As Liam Byrne MP, Chair of the Business and Trade Committee in the House of Commons, said: '...the 'big hole' in the UK's economic defences that was most concerning the US was around export security.'⁴⁷

10.1 Stemming the outward flow of technology

In addition, to stem the outward flow of technology, HM Government should:

- **Strengthen the NSIA.** The NSIA recognised the need to protect UK technology. Byrne has called for tightening the inward investment screening programme and introducing a tougher export control regime.⁴⁸ The law needs strengthening so that *all* investments from the PRC fall within the scope of mandatory notification (this is not as onerous as it sounds, given that Chinese investment represents only 0.2% of the UK's FDI stock). Currently, when a company enters into a collaboration agreement with a British university 'mandatory notification requirements do not apply to acquisitions of assets, including control over intellectual property. However, parties may want to submit a voluntary notification if they believe there is a potential risk to national security.'⁴⁹ Accordingly: 'If the spin-out operates in one of the 17 sensitive areas of the economy specified in notifiable acquisition regulations, there *may* [emphasis added] be a legal requirement to notify the government of the acquisition.'⁵⁰ But

⁴⁶ 'Who are the Joint State Threats Assessment Team?', Secret Security Service MI5 (UK), no date, <https://www.mi5.gov.uk/> (checked: 24/02/2025).

⁴⁷ Lucy Fisher and Peter Foster, 'UK must offer Trump concessions on China to avoid tariffs says trade committee chair', *The Financial Times*, 14/11/2024, <https://www.ft.com/> (checked: 24/02/2025).

⁴⁸ *Ibid.*

⁴⁹ 'National Security and Investment Act: guidance for the higher education and research-intensive sectors', Cabinet Office (UK), 21/05/2024, <https://www.gov.uk/> (checked: 24/02/2025).

⁵⁰ *Ibid.*



responsibility for checking the propriety of investment should not rely on government ‘call-in’; the onus should be on the parties involved. The government’s report on the NSIA notes that, ‘Evidence in the Annual Reports therefore does not suggest that high-risk acquisitions are routinely not being captured by the NARs [Notifiable Acquisition Regulations].⁵¹ This data cannot capture acquisitions of which the Government was not aware.’ This suggests that the government’s market monitoring requires better resourcing.

- **Reinforce the Academic Technology Approval Scheme (ATAS)**, which limits research and doctoral visa applications from countries not on an approved list (EU countries, Switzerland, Norway, other Five Eyes countries, Japan, South Korea and Singapore). One loophole to close is the exemption for individuals who hold a valid Global Talent Visa for employment as a contracted researcher in the UK.
- **Reinforce the Research Collaboration Advisory Team.** RCAT advises universities on the propriety of scientific collaboration with countries not on approved list. Its most recent publication (November 2023) reveals 15 staff and 12 advisers.⁵² This is not commensurate with the scale of their responsibilities or of the challenge. It is essential that RCAT advice is delivered to researchers before they sign contracts with Chinese entities.
- **Establish a scientific advisory board within government focused on Chinese science and technology.** Government departments have their own scientific advisers, but coordination needs raising. Such a board, backed up by a secretariat and by open-source intelligence, should also be able to rule on the appropriateness of partner organisations and individuals. The Investment Security Unit and the National Security Unit for Procurement, both in the cabinet office, might make up the secretariat. It would make sense to move control of the Academic Technology Approval Scheme to the secretariat.
- **Put the PRC on the ‘enhanced tier’ of the Foreign Interests Registration Scheme** under the National Security Act – a move HM Government has so far resisted. This would require UK advisory

⁵¹ ‘Report on the National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021, Cabinet Office (UK), 19/12/2024, <https://www.gov.uk/> (checked: 24/02/2025).

⁵² ‘RCAT Update’, Department for Science, Innovation and Technology (UK), 01/08/2023, <https://www.gov.uk/> (checked: 24/02/2025).



and lobbying companies and individuals working with entities from the PRC to declare such work (all Chinese companies, whatever their ownership structure, must carry out the wishes of the CCP when asked; the reality that, in terms of corporate independence, there is no such thing as a private company in the PRC needs to be rammed home). Such declarations by British companies and individuals would diminish the risk that, whether through naivety or wilful blindness, they might put their own pecuniary interests above those of the nation and future generations.

- **Strengthen the powers of the Advisory Committee on Business Appointments.** ACOBA's remit is to ensure that retiring ministers and senior officials do not prejudice national interests by using inappropriate information and relationships from their time in government. Giving ACOBA teeth would also help to ensure that, faced with hard decisions, ministers and officials would not be swayed by an eye to possible future job offers.
- **Boost the National Strategic Security Investment Fund,** HM Government's corporate venturing arm for dual-use advanced technologies.⁵³ HM Government should also take a golden share in at risk companies.

10.2 Protecting against the inward flow dangerous technologies

Finally, to protect against the inward flow of dangerous technologies, HM Government should:

- **Designate areas of technology where the concept of 'trusted suppliers' must be applied,** in order to mitigate the threats of dependency, disruption and data loss. This could be a further role for a Scientific Advisory Board. This is a complex area, which requires decisions on industrial policy.
- **Make full use of the debarment list set up under the Procurement Act.** HM Government's aim is to prevent companies on the list from participating in government procurement where national security questions arise. It will be managed by a new National Security Unit for Procurement, but implementation has been delayed from

⁵³ 'National Security Strategic Investment Fund', British Business Bank, no date, <https://www.british-business-bank.co.uk/> (checked: 24/02/2025).



October 2024 to February 2025.⁵⁴ It is important that the debarment list is swiftly populated with those Chinese companies which threaten the long-term security of the UK. Foremost are Chinese CIM manufacturers. The CIM example underlines the importance of keeping up with the ‘metastasising’ of Chinese companies as they form companies under other names and jurisdictions in an attempt to get round restrictions, such as might be imposed by the debarment list. Systematic updating of information is essential. It is worth noting that in January 2025, the US put Quectel on the 1260H list, a Department of Defence list of Chinese military affiliated companies, a measure which promotes the exclusion of such companies from doing business with the department.

The scope of this Report does not include a consideration of the possible effects of the second presidency of Donald Trump. However, it is worth noting that a failure to adopt measures to protect the UK’s science and technology in line with the measures recommended – or variants of them – could lead to severe tensions with the incoming US administration, with adverse effects on trade and other important areas of cooperation, for example under the ‘Five Eyes’ arrangements. The case of connected vehicles is the most salient example. The US has recently published ‘Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles’.⁵⁵

⁵⁴ ‘Procurement Act Implementation Delayed until February 2025’, techUK, 12/09/2024, <https://www.techuk.org/> (checked: 24/02/2025).

⁵⁵ ‘Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles’, Department of Commerce (US), 26/09/2024, <https://www.federalregister.gov/> (checked: 24/02/2025).



11. Conclusion

The biggest foreign policy challenge facing the governments of free and open countries in the second quarter of the 21st century is to achieve the correct balance between working with the PRC in trade, investment and shared global problems, while protecting economic and national security. When one side, the CCP, is clear that there is an existential and ideological struggle between political and economic systems, the other can no longer afford to take an outdated or short-term view. A new, if different, cold war has begun. Foreign governments need to disregard the CCP's external propaganda of 'win-win' and 'community with a shared future for mankind'. They should listen to what Xi says when he speaks to the CCP. The threat is not hidden in plain sight: it is in plain sight. Those who are not willing to make the effort to listen, read and understand have only to look at the CCP's dealings with Russia and its support for the Kremlin's offensive against Ukraine – an alliance not a dalliance.

As Xi and others in the CCP have made clear, the main battlefield of this new cold war is science and technology. Foreign governments have belatedly woken up to the threat of over-reliance on the CCP in crucial supply chains, but seem not to have accepted that the triple threats of dependency, disruption and data delivered by future dominance of new technologies require sacrifice and action now. The examples presented by the case of the British microchip company and the issue of CIMs are just two salient cases of complacency, vested interests or failures of understanding. There are many others.

As ever, implementation and action require funding and that is in short supply. But the long-term effects of neglecting economic and national security justify giving a high priority to funding the measures suggested in this Report.

Finally, speed is of the essence. Governments work in units of years: technology (and perhaps sinology) moves in months.



About the author

Charles Parton is Chief Advisor to the China Observatory and a Distinguished Fellow at the Council on Geostrategy.



Acknowledgments

We would like to thank the Coalition on Secure Technology (CST) for their partnership in producing this paper. The CST is a cross-party campaign which works to raise awareness of the threat posed to our economy and our way of life through technology produced by openly or potentially hostile states. Chaired by Graeme Downie MP (Labour) and backed by leading China expert Charlie Parton, the CST aims to raise awareness amongst the public, policy makers, and politicians of the risks associated with such technology and our increasing dependence on Chinese suppliers and equipment – emphasising the importance of the UK mitigating these risks for the future.



About the Council on Geostrategy

The Council on Geostrategy is an independent non-profit organisation situated in the heart of Westminster. We focus on an international environment increasingly defined by geopolitical competition and the environmental crisis.

Founded in 2021 as a Company Limited by Guarantee, we aim to shape British strategic ambition in a way that empowers the United Kingdom to succeed and prosper in the twenty-first century. We also look beyond Britain's national borders, with a broad focus on free and open nations in the Euro-Atlantic, the Indo-Pacific, and Polar regions.

Our vision is a united, strong and green Britain, which works with other free and open nations to compete geopolitically and lead the world in overcoming the environmental crisis – for a more secure and prosperous future.

About the China Observatory

This Report is part of the Council on Geostrategy's China Observatory. The China Observatory seeks to watch, monitor and evaluate the evolution, behaviour and actions of the Chinese Communist Party. Together with experts and legislators, the Observatory aims to guide HM Government in the formulation of a coherent 'China policy' through research-led, non-partisan analysis from a British vantage point.

[THIS PAGE IS INTENTIONALLY LEFT BLANK.]



Council on Geostrategy **CHINA OBSERVATORY**



Dedicated to making Britain, as well as other free and open nations, more united, stronger and greener.

ISBN: 978-1-914441-96-7

Address: 14 Old Queen Street, Westminster, London, SW1H 9HP

Phone: 020 3915 5625

Email: info@geostrategy.org.uk

© 2025 Council on Geostrategy

Disclaimer: This publication should not be considered in any way to constitute advice. It is for knowledge and educational purposes only. The views expressed in this publication are those of the author and do not necessarily reflect the views of the Council on Geostrategy, the views of its Advisory Board, or the views of the China Observatory's Advisory Council.

Please do not print this document; protect the environment by reading it online.

Geostrategy Ltd., trading as Council on Geostrategy, is a company limited by guarantee in England and Wales. Registration no. 13132479. Registered address: Geostrategy Ltd., 14 Old Queen Street, Westminster, London, SW1H 9HP.

New geostrategic thinking for a more competitive age

<https://www.geostrategy.org.uk>