Council on Geostrategy

Policy Paper
Geostrategy Programme
No. GSPPP02
March 2024

Chinese cellular (IoT) modules: Countering the threat

By *Charles Parton*

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

[This page is deliberately left blank.]

Contents

Foreword

As new and cutting-edge technologies continue to appear and shape modern society, free and open countries across the world are right to be concerned about adopting those developed and managed by supplier nations which may not be fully trusted. In the case of the People's Republic of China (PRC), multiple countries already have banned its state-championed telecommunications giant Huawei, and the United States is edging closer to legislating a ban on TikTok amid concerns over data and the manipulation of content.

These stories and companies grab the headlines, which makes sense given their size and the potential immediate impact on citizens' lives. However, a greater challenge may loom in cellular (internet of things) modules produced, and their firmware subsequently managed, in the PRC.

As this Policy Paper by Charles Parton demonstrates, the manipulation of this technology could have severe ramifications for the functioning and security of the United Kingdom, as well as its allies and partners. This Paper is an important contribution to a debate which should be aired more openly within governments across the world, and provides insights which are not just relevant to Britain, but any nation attempting to address gaps in its approach to the PRC.

James Rogers

Co-founder and Director of Research, Council on Geostrategy

Executive summary

- The spread of new technologies, the erosion of the distinction between civil and military technology and the penetration of technology into all aspects of life mean that the definition of critical national infrastructure (CNI) is broadening.

- Cellular (internet of things or IoT) modules (CIMs) are becoming ubiquitous components, vital to everyday items, such as routers, smart meters or cars, as well as to the biggest logistics and manufacturing systems and processes. They are a gateway through which data flows in both directions.

- Trust in the manufacturers of CIMs is vital because manufacturers have the ability through firmware over-the-air updates to install malware.

- The Chinese Communist Party (CCP) is intent on gaining a monopoly of supply of CIMs. If it succeeds, the threat to free and open countries is threefold: the CCP would capture vast amounts of data and weaponise it; the CCP would gain the capability to turn off systems, a potent form of economic warfare; and the CCP could pressure foreign governments into changing policies under threat of interruption to the supply of CIMs.

- By way of examples of the threat, this Policy Paper looks at the dangers of a Chinese monopoly of supply in the fields of vehicles, smart meters and routers. The current debate on imports of Chinese electric vehicles largely misses out the important national security angle.

- Responsible governments should not sit back and allow the CCP to threaten longer-term economic and national security. To trust that the CCP will not exploit any advantage it gains would be beyond naïve. The People's Republic of China is known to be scoping out foreign countries' CNI. CIMs provide an entry point.

- Awareness in governments of the problem of CIMs and of the main Chinese protagonists is low (names such as Quectel and Fibocom should be as familiar as Huawei, Hikvision or TikTok).

- 'Rip and replace' is not a feasible strategy, except in a limited number of defence and security fields. But governments should take measures urgently to prevent an increase in Chinese CIMs embedded in their CNI.

- The United Kingdom and the United States are beginning to consider measures to limit the use of Chinese CIMs. India is clear about the threat. The European Union lags behind.

- This Paper ends with a series of recommendations, which focus on:

    - Carrying out an audit of Chinese CIMs in CNI;
    - Carrying out research and awareness training;
    - Establishing a centre of government expertise able to advise all departments and help with security plans;
    - Legislating and implementing laws to exclude Chinese CIMs from all government procurement;
    - Banning government departments from using vehicles with Chinese CIMs and prohibiting private vehicles with Chinese CIMs from entering military and other sensitive areas;
    - Excluding Chinese CIMs from health services' equipment and systems (to comply with data protection requirements);
    - Excluding Chinese CIMs from consumer telecommunications products such as routers; and,
    - Legislating to ban Chinese CIMs in all CNI (under an updated definition of CNI).

1.0 A shrinking distinction between economic security and national security

Over time national security and economic security converge into one. Economic security – the ability to keep an economy going under the threat or actuality of interference or disruption by a hostile power – underpins national security and its components (politics, food, energy, military, environment and data).

The backbone of economic security is critical national infrastructure (CNI). At the very least, that must be proofed against those considered enemies of the state and society.

A broadening definition of CNI

For much of the 20th century the definition of CNI bumbled along. Obvious areas included power generation and transmission, transport (railways, airports, seaports), food infrastructure, and data transmissions systems (telephones and telecommunications). Recent decades have seen the increasing importance of telecommunications, the internet, information technology, and the transmission of ever-increasing amounts of data. A third age is now dawning, of the internet of things (IoT), artificial intelligence and quantum computing.

Three trends are contributing to a wider definition of CNI:

1. The ubiquity of the new sciences and technologies, now present inside nearly all homes and organisations;
2. The erosion of the distinction between the civil, military and surveillance/repression uses of technology, which allows a hostile power to weaponise previously non-threatening appliances or components; and,
3. The power of aggregated data (one person's data may not matter much, but millions of peoples' data can be used to make important economic, industrial, social, security or other tools, whether for benign or malign purposes).

'New' CNI includes modern cars (now in essence computers/smartphones on wheels) and charging points, smart

meters, routers for internet traffic, remote medical equipment, consumer satellite devices, payment systems, and more.

What makes them CNI is the presence within them (also in older forms of CNI) of cellular (internet of things or IoT) modules (CIMs). Worryingly, few people are aware of their existence, capabilities or importance to everyday functions.

2.0 What is a cellular IoT module

CIMs are electronic wireless components embedded in larger devices or sub-units rather than finished items, such as CCTV cameras, drones and utility meters. They connect to the internet in the same way as a mobile phone does over the cellular network. CIMs enable devices to be connected externally to other devices or systems, and they collect data for internal remote servers.

CIMs are not semiconductors or sim cards, although they contain both (an 'e-sim'). They have processor units for power, modem and applications, filters, amplifiers, antennae and memory. They are not necessarily hi-tech, although the spread of 'edge-computing' means an increasing ability to do tasks previously carried out away from the systems in which CIMs are embedded.

CIMs are ubiquitous. At the end of 2022 there were an estimated 19.8 billion in use.[1] By the end of 2025 that figure is projected to rise to 30.9 billion.[2]

Industries, agriculture, telecommunications, logistics and other systems rely on them to monitor, to help control and to improve processes essential to the functioning of a modern economy and society. Without CIMs sophisticated modern cars, smart (and efficient) power grids, efficient mobile payment systems, complex production lines, clever security and access systems, invaluable hospital services, and much more could not function. CIMs are, in effect, communication computers – the gateway to systems.[3]

The user must trust the manufacturer

The manufacturer has written in large amounts of code. CIMs are also required by cellular service providers to include the capability to update software remotely. This is essential for fixing problems, enhancing performance, adjusting to mobile network operator settings, or implementing security patches. These updates, known as FOTA

[1] Josh Howarth,'80+ Amazing IoT Statistics (2024-2030)', *Exploding Topics*, 03/11/2023, https://explodingtopics.com/ (checked: 18/03/2024).
[2] *Ibid.*
[3] Charles Parton, 'Cellular IoT modules – Supply Chain Security', OODA Loop, 02/2023, https://www.oodaloop.com/ (checked: 18/03/2024).

(firmware- over-the-air), occur behind the scenes without the end-user's knowledge – similar to updating the operating system or applications on a smartphone.

This lifelong umbilical cord allows manufacturers significant insights into their customers' equipment, processes and data – even more so when manufacturers analyse data for customers, a service increasingly being offered. Users must trust manufacturers. Firmware updates could contain malware, and it is not possible to check every update throughout the life of the module.

3.0 Why are Chinese CIMs a threat?

It is first necessary to consider the broader threat posed by the Chinese Communist Party (CCP) to free and open countries.[4] As Xi Jinping, General Secretary of the CCP, says, 'The Party leads everything.' Chinese manufacturers of CIMs are no exception. Security laws oblige them to cooperate with CCP instructions.

Xi's aim is for the People's Republic of China (PRC) to become a 'great modern socialist country which is rich, strong, democratic, cultured, harmonious, and beautiful' by mid-century. In Xi's words, that means: 'China becomes the leading country in comprehensive national strength and global influence' and that 'the Chinese nation will stand mightily among the world of nations'.[5] In sum, his aim is for the PRC to replace the United States (US) as the leading superpower, and to reorder global governance better to suit CCP interests and values.

To achieve this, Xi does not intend to use force, although a modernised, effective People's Liberation Army is a useful tool of menace. Amongst the most important methods are: the domination of cutting-edge sciences and technologies; the amassing and control of data; and the creation of economic and other dependencies. This last example is not just a matter of minerals, materials and resources, such as rare earths, lithium, gallium, germanium. Dependencies relating to new technologies and industries, and components and systems, are every bit as dangerous. Better to strangle an enemy's economy or disable its CNI than to resort to the uncertainties and losses of war – or threaten to. It is in this context that economic security blends into national security.

Given the ubiquity and crucial nature of CIMs, depending on the CCP for supply would be very dangerous. The party has designated cellular modules as one of its key industries.[6] It is setting out to ensure

[4] Charles Parton, 'Is China a threat?', Council on Geostrategy, 16/03/2023, https://www.geostrategy.org.uk/ (checked: 18/03/2024).
[5] Xi Jinping, *The Governance of China* (Beijing: Foreign Language Press, 2014), vol. 2, p.23.
[6] In 2009, the Chinese government initially designated IoT as a strategic sector for development, and followed with significant financial support toward the sectors' development. In 2012 the Ministry of Industry and Information Technology referred to the IoT as a 'strategic high ground'. In the 13th Five Year Plan, which covered 2016-20, the section on digital and telecommunications development included direct efforts aimed at boosting IoT chip design and manufacturing. This was also in support of 'information flow' along the Belt and Road

that Chinese companies gain a monopoly of supply. By the fourth quarter of 2022, they held over 60% of the global market, and represented some of the biggest companies (Quectel 38.5%, Fibocom 7.5%, Sunsea AioT 5.3%, China Mobile 5.2%, and MeiG 4.3%).[7] The main Western companies were Telit (US, 6.3%), Thales (France, 5.7%, now merged with Telit, to become Telit Cinterion), Sierra Wireless (Canada, 4%) and Ublox (Switzerland, 3.2%).[8] Japan's Resenas and Korea's SJI had smaller shares.

The Chinese party-state ensures that its 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, and other state support. Quectel is particularly aggressive in its pricing, to the extent that Western competitors believe that its CIMs are being sold at between 15-25% below what it costs to manufacture in the PRC.[9] Another well-worn path is to buy up competitors. For example, in 2023 Fibocom bought Luxembourg-based Rolling Wireless.[10]

The intention is to drive out foreign competition, including through underhand targeting of competitors' main clients.

The big three threats

Quectel, Fibocom, Sunsea and other Chinese companies have no choice but to obey the diktats of the CCP. Chinese security laws ordain so, but irrespective of laws, no management could turn down a CCP instruction. No matter their ownership structure, companies must function as tools of the party when requested.

If Chinese companies were to succeed in gaining a monopoly of supply of CIMs, free and open countries would face three threats:

Initiative. This continued in the 14th Five Year Plan. The development of the IoT was intended to support a range of industries including agriculture, city infrastructure, customs and border posts, and manufacturing. See: John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green, Jonathan Ray and James Mulvenon, 'China's Internet of Things', SOSi, 24/10/2018, https://www.uscc.gov/ (checked: 18/03/2024).

[7] 'Cellular IoT Module Market Update', *IoT Business News*, 25/01/2023, https://iotbusinessnews.com/ (checked: 18/03/2024).

[8] *Ibid*.

[9] Author's interview with two separate industry insiders.

[10] Satyajit Sinha, 'Cellular IoT module & chipset market 2023: 18% decline due to destocking and softening demand in key segments', *IOT Analytics*, 19/12/2023, https://iot-analytics.com/ (checked: 18/03/2024).

The CCP could put pressure on governments to change policies – in any field – by threatening to withhold CIMs. Such pressure might be direct or delivered through a nation's companies, which would lobby for relief by changing policy. In practice, knowing that restrictions could be applied would lead governments into a pre-emptive policy kowtow.

CIM firmware updates with embedded malware could degrade or destroy the performance of industrial systems, CNI, or other economic entities. It is worrying to note that in the past year, US authorities have become concerned about Chinese cyber attacks which appear to be scoping out CNI. Brandon Wales, the Executive Director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, talked of Chinese attempts 'to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict'.[11] According to officials, hackers 'mask their tracks by threading their attacks through innocuous devices such as home or office routers before reaching their victims.'[12]

The acquisition by the CCP of massive amounts of data. This year the Five Eyes intelligence alliance offered open advice on combating hacking.[13] They noted that hackers often get round defences by using legitimate tools, making their attacks resemble normal network activity.[14] The use of a Chinese CIM is in effect an invitation into a system, because CIMs are the gateway to computers; they are designed to allow an interchange of information.

Examples of how such threats may play out if China monopolises CIM supply

Vehicles

Modern vehicles can be described as computers on wheels. Access to those computers is through the CIM enabled gateway. It is possible to send instructions buried in firmware and software updates to immobilise vehicles, just as John Deere did when the Russians stole

[11] *Ibid.*
[12] Ellen Nakashima and Joseph Menn,'China's cyber army is invading critical U.S. services', *The Washington Post*, 11/12/2024, https://www.washingtonpost.com/ (checked: 18/03/2024).
[13] 'Five Eyes intelligence partners launch outreach drive to secure innovation', MI5, 17/10/2023, https://www.mi5.gov.uk/ (checked: 18/03/2024).
[14] *Ibid.*

agricultural machinery from Ukraine.[15] Manufacturers of CIMs, not just vehicle operators or makers, could do the same. This presents a big threat to the UK's or other European countries' economic security. As Professor Jim Saker, President of the Institute of the Motor Industry, warned, the Chinese electric (or conventional) cars flooding into Europe 'could be immobilised remotely by officials in China'.[16] This 'threat of connected electric vehicles flooding the country could be the most effective Trojan horse that the Chinese establishment has, if Beijing wanted to destabilise the UK economy.'[17] Remote updating through the CIMs would allow changes to a car's behaviour. It would not take many simultaneously immobilised vehicles to paralyse London traffic. Or a hostile power could choose to immobilise all government or all defence vehicles.

Just as serious is the threat of data collection from vehicles or charging stations. Many modern cars report performance and geolocation details in real time. Knowing the location or plotting the movements of every government or defence vehicle represents a serious security threat. It is possible to piggyback on cars' cameras, now sufficiently high quality to allow facial recognition of people on the streets. This is not science fiction: Tesla engineers have been sacked for laughing at films and audio from private citizen's cars.[18] In January 2023 iNews reported that the British security services had stripped down a government car because of data emanating from its 'e-sim' (i.e. the CIM) to the PRC.[19] Equally dangerous is plugging a mobile phone into the audio management system of a car with a Quectel or Fibocom CIM. Once synchronised, the phone's data can be sent back to the Chinese manufacturers, in effect back to the PRC. Given advances in technology, such threats, including the transmission of conversations (such as ministers talking by phone in cars) will only become more serious.

[15] Olexsandr Fylyppov and Tim Lister, 'Russians plunder $5M farm vehicles from Ukraine – to find they've been remotely disabled', *CNN*, 01/05/2022, https://edition.cnn.com/ (checked: 18/03/2024).
[16] Jonathan Ames, 'Chinese electric cars "could bring UK roads to a standstill"', *The Times*, 30/07/2023, https://www.thetimes.co.uk/ (checked: 18/03/2024).
[17] *Ibid*.
[18] Steve Stecklow, Waylon Cunningham and Hyunjoo Jin, 'Tesla workers shared sensitive images recorded by customer cars', *Reuters*, 06/04/2024, https://www.reuters.com/ (checked: 18/03/2024).
[19] Richard Holmes,'Hidden Chinese tracking device "found in UK Government car" sparks national security fears', *iNews*, 06/01/2023, https://inews.co.uk/ (checked: 18/03/2024).

Smart meters and grids

Smart meters contain CIMs. According to an engineer, it would take little more than a day to write software which could be sent to all smart meters instructing them to behave in a certain way at a certain time, when demand for electricity was very high.[20] This could unbalance the grid (smart meters are designed to help power generation companies supply more efficiently) and potentially take it down, with repairs likely to take many months.

Routers/Customer Premise Equipment (CPE)

Governments congratulate themselves on shutting the front door to exclude Huawei from telecommunications. Yet they have left the back door and windows open. Routers/CPE which contain Quectel, Fibocom or other Chinese CIMs are vulnerable. While governments may protect their departments, the chances are minimal that ministers and officials working from home are fully protected.

There are two threats. First, via the CIM the router could be shut down, blinding end users who need internet access. This could prevent key workers from doing their jobs. Second, routers with Chinese CIMs would enable the CCP to access data and conversations. The damage in the case of individuals might be limited unless they are important officials. But the aggregation of data constitutes a bigger threat. It would, for example, enable the Chinese intelligence services to sift out those who would make useful intelligence targets, as well as to understand their vulnerabilities. But equally, in terms of economic security, CIMs in routers could facilitate the plundering of commercial and technological secrets of British companies.

[20] Author's conversation with an engineer working for a company producing CIMs.

4.0 Strategic challenges

There is little direct or open evidence – the British government car described above may be an exception – that the CCP has been extracting data via CIMs. If British and allied intelligence services have such evidence, they have not publicised it. However, the CCP has an extraordinary track record of exploiting the weaknesses in targets' defences and stealing the data of foreign governments, defence systems, commercial companies, and individuals. Chinese CIMs in target systems are a profound weakness, ripe for exploitation.

Similarly, there is no evidence of the second threat, that the CCP has deliberately degraded or shut down foreign systems. But recent reports suggest that the CCP is preparing the ground by scoping out the US' and other countries' CNI against the day that the weapon could be used in non-kinetic warfare. As Christopher Wray, the Director of the Federal Bureau of Investigation, said when giving evidence to a congressional committee in January: 'There has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure – our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems – and the risk that poses to every American requires our attention now.'[21]

On the third threat – policy leverage – Chinese CIM manufacturers have yet to gain a monopoly of supply. The CCP is thus not yet in a position to impede supply to an effective degree.

What is certain is that the technology allows them to weaponise CIMs as described. Furthermore, the CCP sees itself as engaged in an existential struggle in which its version of socialism must defeat Western capitalism.[22]

Responsible governments should not sit back and allow the CCP to threaten longer-term economic and national security. To trust that the CCP will not exploit any advantage it gains would be beyond naïve.

[21] Christopher A. Wray, 'Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party', Federal Bureau of Investigation, 31/01/2024, https://www.fbi.gov/ (checked: 18/03/2024).
[22] Charles Parton, 'Is China a threat?', Council on Geostrategy, 16/03/2023, https://www.geostrategy.org.uk/ (checked: 18/03/2024).

A lack of awareness in free and open countries

Awareness is low, both of the wider threat from a different economic system, which is without precedent in its effectiveness and ruthlessness, and from the particular threat from Chinese CIMs. In the author's experience of talking to politicians and civil servants in the United Kingdom (UK), US, European Union (EU) and India, few have heard of CIMs. Security services are surely aware, but they appear not to have confided their worries to policy makers.

A second problem is the reluctance of those in the industry and those who consume CIMs to speak out. For some, it is the fear that Chinese suppliers of other components or materials will withhold supplies. For others it seems a long-term problem, one which does not affect short-term share performance. For some businesses owned by venture capitalists, the explanation appears to be an unwillingness to cause controversy and affect the value of a company which will eventually be sold. There are also some Western companies deliberately promoting Quectel, for example, because they earn much of their profits in the PRC.[23] Quectel also pays its licence fees upfront.[24]

Some signs of awakening

Some Western governments have begun to react to calls to wake up – even if late in the day.

UK. A start has been made by the passing of the Procurement Act in October 2023. Ministers initially turned down suggested amendments which would permit the exclusion of Chinese CIMs from government procurement. However, they relented and the Act has set up a debarment list. Companies bidding for government contracts may not use any supplier which has been placed on the debarment list. The act also established a National Security Unit for Procurement (NSUP) in the Cabinet Office to implement and monitor the list. The debarment list goes live in October 2024. A minister must review the list regularly. The law will send a strong and wider message on the security of using Chinese CIMs – but only if one of the first actions of the NSUP is to place Chinese CIM manufacturers on the debarment list and enforce a ban.

[23] Author's interview with an industry insider.
[24] *Ibid.*

US. In August 2023 the House Select Committee on the Strategic Competition Between the US and the CCP wrote to the Federal Communications Commission (FCC) requesting to know what actions it might be considering to deal with the threat of Chinese CIMs.[25] The FCC in turn wrote to eight government departments (State, Defence, Homeland Security, Justice, the Federal Acquisition Security Council, and the three intelligence agencies) welcoming 'the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List.'[26] The conclusions and possible actions have yet to emerge. In January 2024 the House Select Committee on the CCP wrote to the departments of defence and treasury requesting that they put 'Quectel on the Department of Defence's list of Chinese Military Companies (1260H list) and the Department of Treasury's Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List).'[27] It is also likely that the 2024 National Defence Authorisation Act will include a provision to ban Chinese CIMs from Department of Defence procurement, in much the same way as the UK's Procurement Act may operate. Recent announcements by Joe Biden, the American President, into an investigation into the national security implications of Chinese connected vehicles and worries about communications devices found in Chinese cargo cranes show a raised concentration on CIMs (even if they are not specifically mentioned in reports, the threat of their presence is implied).[28]

EU. Neither the EU nor its member states appear to have considered the question of Chinese CIMs.[29] This is surprising, given that

[25] Mike Gallagher and Raja Krishnamoorthi, 'Letter to Jessica Rosenworcel', Select Committee on the Chinese Communist Party (US), 07/08/2023, https://selectcommitteeontheccp.house.gov/ (checked: 18/03/2024).
[26] The collection of letters written by the Federal Communication Commission can be found here: https://docs.fcc.gov/ (checked: 18/03/2024).
[27] The 1260H list is designed to stop the Department of Defence using companies on the list on the grounds of national security. Implementation has hitherto been disappointing. The Treasury list sets down companies in which American entities should not invest. Although the list does not ban federal dollars being spent on contracts with those companies, the reputational damage of doing so when investment in them is prohibited should be effective in preventing such contracts being signed.
[28] On Chinese vehicles, see: 'Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles', Department of Commerce (US), 29/02/2024, https://www.commerce.gov/ (checked: 18/03/2024) and on Chinese cargo cranes, see: Dustin Volz, 'Espionage Probe Finds Communications Device on Chinese Cranes at U.S. Ports', *The Wall Street Journal*, https://www.wsj.com/ (checked: 18/03/2024).
[29] The author's recent discussions in Brussels confirmed this.

the Commission is most concerned by the threat of Chinese electric vehicles being dumped on the European market. Aside from the subsidy concerns, the strongest argument for restricting imports is on national security grounds, i.e. the threat from CIMs.

India. India has been forthright in banning Chinese technology (for example, it refused investment from Chinese car manufacturer BYD and has banned TikTok). Government officials, think tanks and businesses are fully aware of the problem of CIMs. However currently, Chinese CIM manufacturers have nearly 90% of the Indian market.[30] Action to reverse this is being considered.

[30] Author's conversations with officials in Delhi.

5.0 Recommendations

'Rip and replace' is not a viable option because too many Chinese CIMs are already in place. The exception is for CIMs in military, intelligence and other sensitive installations. The broad strategy must be to restrict future use of Chinese CIMs and to promote gradual replacement with CIMs produced by companies not controlled by the PRC (there are many alternatives). Over time this will cleanse systems. Meanwhile the following actions are necessary:

Audit. Swiftly establish in which important CNI and in which sensitive systems (defence, intelligence etc.) Chinese CIMs are installed, so that the current risk can be gauged and immediate remedial action carried out.

Research and awareness raising. Broaden understanding of the threat of CIMs to economic and national security, as well as to the values and data of free and open countries. Conduct awareness training within government departments, particularly with regard to procurement practices (see legislation below).

Planning. Ensure that there is a centre of expertise on economic security, with oversight of all government departments' performance in that area, which is also able to give advice. All departments should include CIMs in their information security plans.

Procurement. **For the UK**: ensure that Chinese CIM companies are put on the Procurement Act's debarment list in October 2024. In order to keep up to date with developments (Quectel, for example, is already setting up an 'American' company IKOTEK, which is wholly owned by Quectel, but seems to be designed to get round future restrictions), the NSUP should buy open source intelligence from specialist companies. IKOTEK and similar Chinese companies under foreign guise should also be put on the debarment list. **For other countries**: legislate immediately to prevent Chinese CIM companies' participation in government procurement.

Ban government departments from using vehicles with Chinese CIMs. Private vehicles with Chinese CIMs should be prohibited from entering sensitive areas (note that the Chinese apply similar bans in the

PRC: Tesla vehicles are prohibited from entering military bases or places being visited by Xi).[31]

Ban Chinese CIMs from health services' equipment and systems. There may be GDPR considerations if Chinese CIMs give access to individuals' medical data to companies in the PRC and to the CCP authorities.

Legislate or implement legislation to exclude Chinese CIMs from consumer products such as routers and other telecommunications. For the UK: implement the Product Security and Telecommunications Infrastructure Act 2022 provisions relating to security (e.g. Chapter 1, sections 16, 23, 30 and 66).[32]

Prepare and pass legislation to ban Chinese CIMs in all CNI. This first requires governments to redefine what it considers to be CNI in the light of science and technology developments as well as CCP intentions.

[31] 'Tesla cars banned from China's military complexes on security concerns', *Reuters*, 19/03/2021, https://www.reuters.com/ (checked: 18/03/2024).
[32] 'Product Security and Telecommunications Infrastructure Act 2022', UK Public General Acts, 2022, https://www.legislation.gov.uk/ (checked: 18/03/2024).

About the author

Charles Parton OBE is a James Cook Associate Fellow in Indo-Pacific Geopolitics at the Council on Geostrategy. He spent 22 years of his 37-year diplomatic career working in or on China, Hong Kong and Taiwan. In his final posting he was seconded to the European Union's Delegation in Beijing, where, as First Counsellor until late 2016, he focussed on Chinese politics and internal developments, and advised the European Union and its Member States on how China's politics might affect their interests. In 2017, he was chosen as the Foreign Affairs Select Committee's Special Adviser on China; he returned to Beijing for four months as Adviser to the British Embassy to cover the Communist Party's 19th Congress.

Acknowledgments

The author would like to thank the Coalition on Secure Technology (CST) for their support. The CST, chaired by Baroness Natalie Evans, was established to highlight the threat to UK economic and national security from Chinese CIMs.[33]

[33] For more on the CST, see: 'Who we are', The Coalition on Secure Technology, No date, https://cim-coalition.co.uk/about/ (checked: 18/03/2024).

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.

Notes

Notes

[This page is intentionally left blank.]

Council on Geostrategy

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

ISBN: 978-1-914441-63-9

Address: 14 Old Queen Street, Westminster, London, SW1H 9HP
Phone: 020 3915 5625
Email: info@geostrategy.org.uk