The Threat from Chinese cellular (IoT) Module Companies with reference to the Automotive Industry

Written testimony submitted to the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party

Introduction

In most technological sectors, governments have the difficult task of reconciling four often competing needs: national security, economic prosperity, environmental factors, and public opinion. The rise of China, the omnipresence of new technologies in most spheres of life, and the dissolving distinction between military and civilian uses of technology have complicated this task, nowhere more so than in the automotive sector.

The author has set out the role of cellular (IoT) modules (CIMs) and the nature of the threats which domination or monopoly of their supply by China poses in more detail in earlier papers.[1] This report looks at Chinese intentions to dominate the connected vehicles (CVs) sector. But what is set out relating to CVs applies equally to manufacturing, logistics, agriculture, telecommunications, energy grids, pipelines, home appliances, security and most other sectors.

The Chinese Communist Party's (CCP) aims to gain a monopoly of this vital component. Given the role CIMs in every sector of a modern economy, not just to connected vehicles, this potential supply dependency is more serious than China's domination of the supply of rare earths. CIMs are the gateway to almost all modern systems. Latest estimates project that by 2029, CIM connections could reach 7 billion.[2]

Today, China is the source of around 69 per cent of global CIM shipments, which is a proxy for CIM connection. It is driving out western competition through subsidies and other support. Already western players are being sold to Chinese competitors (Sierra Wireless of Canada sold its automotive CIM production line, ultimately to Fibocom). Others have shut their CIM division (u-Blox of Switzerland).

This report concentrates on three threats posed by Chinese CIMs in the automotive industry: supply dependency and leverage; disruption or destruction of operations; and capture of data. **It bears constant repetition that what applies in the automotive sector is equally important in almost all other sectors of the economy and society.**

The report also focuses on actions being taken by Chinese companies to get round possible defensive measures which may be advanced by countries to protect their national and economic security. In particular, it is vital to understand that even if a CIM manufacturer is established in the United States or Europe, if it uses Chinese technology and depends on continued support from China, the same three threats of dependency, disruption and data egress remain.

The report ends with recommendations for countering the threat.

---

[1] See Charles Parton:
https://cim-coalition.co.uk/wp-content/uploads/2024/12/The-Infrastructure-Threat-from-Chinese-Cellular-IoT-Modules-CIMs.pdf (2 page report);
https://cim-coalition.co.uk/wp-content/uploads/2024/03/Chinese-CIMs-Countering-the-Threat.pdf (medium length report);
https://www.oodaloop.com/wp-content/uploads/2023/02/Cellular_IoT_Paper_JAN_Master_PDF.pdf (long report)

[2] https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

What is a cellular (IoT) module?

Cellular modules are about the size of a thick credit card. They contain processors, memory, antennae and an e-sim to link to the internet. They are, in effect, the gateway to connected systems enabling modern equipment, processes and systems to function. They are vital, because they continually transmit data. They monitor, control, and update systems.

The role of the CIM in connected vehicles is crucial. It is both the hero and the villain of the piece. Modern cars, vans, trucks are now basically 'laptops on wheels'. On board computers control the functioning of the engine, the audio and information systems, sensors, cameras, LiDAR (Light Detection and Ranging, which uses laser light to bounce off objects to create detailed 3D mapping of a vehicle's surroundings, in order to avoid hazards and to enable semi-autonomous or autonomous driving), and more. CVs are mobile surveillance machines, both outside and inside the vehicle.

It is worth repeating that vehicles are just one area where Chinese CIMs are a threat to critical national infrastructure. Cranes, routers, grids, pipelines, payment terminals, building control systems, logistic networks, manufacturing processes and more rely on CIMs.

The three threats of a Chinese monopoly of CIM supply: "Rare Earths 2.0".

Fifteen years ago, the CCP determined that the internet of things (IoT) was a vital interest, which it would seek to dominate or 'seize the commanding heights'.[3] Using its playbook of subsidies, cheap land, preferential financing, and other methods[4] – but also highly efficient manufacturing – it is seeking to drive out American, European, Japanese and Korean companies from the market and to establish a monopoly of the supply of CIMs.

It is not hard to see what would happen if they were to be successful. The software in vehicles (or other systems using the IoT) is being continually updated – via the CIM – but so is the firmware of the CIM itself, through firmware over the air (FOTA) updates. If a vehicle has a Chinese CIM – or three, in some cases, such as Amazon delivery vans – those updates would come from China. This is the same as allowing China access to your laptop. It is not possible to inspect every update for malware. If the CCP succeeds in forcing out of production American and other manufacturers of CIMs, this gives rise to three threats (in order of seriousness):

1. **Dependency.** Given the crucial importance of CIMs to most economic activity, a CCP monopoly would create a more powerful supply dependency than one on rare earths. In today's age of economic coercion, the CCP could leverage this in many ways: "Western government, we don't like your Taiwan policy, your trade policy or your national security exclusions. Please think again, or the supply of CIMs will dry up." Liberal democracies have belatedly learnt the power of the CCP's weaponisation of the supply of rare earths. The threat from CCP control of CIMs would be broader in application. Welcome to "Rare Earths 2.0".[5]

[3] See for example Xi Jinping's speech of 28 May 2018: "New-generation information technologies, represented by artificial intelligence, quantum information science, mobile telecommunications, the Internet of Things, and blockchain are accelerating breakthrough applications." Xi urged scientists to 'actively seize the commanding heights of technological competition and future development.'
The speech was published in Qiushi (http://www.qstheory.cn/dukan/qs/2021-03/15/c_1127209130.htm) and a translation is available at: https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/
The Internet of Things was mentioned as a priority area as early as the 'Made in China 2025' policy promulgated in 2015. https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf

[4] One foreign manufacturer commented to the author that the majority of the cost of a CIM was in the chipset, that foreign companies were known to be getting as good a price for the chipsets as Chinese companies, and yet Chinese CIMs were persistently around 20% cheaper.

[5] See Charles Parton, 'We must face China's rare earths 2.0 moment'. https://www.fdiintelligence.com/content/0e92b05f-f970-41be-aa07-c81bdc9c8895

2. **Disruption or destruction.** Regular FOTA updates cannot all be screened individually. At a time of tension or war, malware could be introduced into the CIM to bring to a halt or crash connected vehicles - or cranes, routers, grids, pipelines, payment terminals or other aspects of critical national infrastructure. Why would the CCP ever fight the US and its allies, when it can simply turn off their systems? How could missiles move from factory to base, if trucks or railways have been turned off. This is eminently possible: when the Russians stole John Deere agricultural machinery from Ukraine, John Deere turned it off – via the CIM. But equally, that need not have been the vehicle manufacturer: it could have been the CIM manufacturer. And as Microsoft has revealed, the Chinese have already spent five years mapping out US critical national infrastructure (operation Volt Typhoon) and embedding viruses to be activated during crises.[6]

3. **Data exfiltration.** With so many sensors, cameras, LiDAR etc on vehicles and other connected devices, significant data theft is a reality. A Chinese vehicle manufacturer, for example, can download much, if not most, of the data from a smart phone plugged into the audio control system. Tesla engineers have been sacked for laughing at video recordings taken from private cars.[7] While personal privacy is a concern, data exfiltration can also have national security implications. In 2022, the UK security services stripped down the Prime Minister's car because data was passing through the CIM to China.[8] Connected vehicles in sensitive defence and intelligence bases could be used to build a detailed picture of their layout. Camera data combined with other data could lead to facial recognition of personnel. In wartime, the cars of crucial military, intelligence or government personnel could be identified and forced off the road or into a collision.

It is important to emphasise that these threats apply not just to Chinese manufactured vehicles, but to any vehicle, American or European, *which contains a Chinese CIM*. **They also apply to any CIM manufactured in the US or Europe which relies on Chinese technology and algorithms.**

More widely, the three threats apply in other sectors of critical national infrastructure besides CVs.

Dealing with the metastasising threat of Chinese CIMs

Awareness of these threats is growing, but slowly. In January the US government put Chinese CIM producer Quectel — the industry's biggest player — on its 1260H list, which identifies Chinese military firms subject to heightened national security. The Department of Commerce also put out a connected vehicle rule with three components: it banned PRC manufacturers from selling connected vehicles in the US; banned the sale of vehicles containing Chinese connectivity after 2026; and banned the sale of vehicles with Chinese components which enabled connectivity after 2029.[9]

Chinese companies are taking prophylactic action, attempting to sidestep future restrictions by 'metastasising' to form US or European companies and joint ventures, which are still owned by China or by Chinese-controlled interests.

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
[7] https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/
[8] Although the original journalist's report of the data leak does not mention that the vehicle was the UK Prime Minister's car, that fact was confirmed to the author by a high-level government source
https://inews.co.uk/news/hidden-chinese-tracking-device-government-car-national-security-2070152
[9] https://www.bis.gov/connected-vehicles

This metastasising — it is indeed a cancer — does not diminish the three threats, unless Chinese CIM manufacturers in licensing their IP hand over their source codes to foreign manufacturers, and play no part in future development of the technology, FOTA updates, and the manufacturing processes. It is not possible to inspect every update for malware. Therefore, the supply of CIMs must come from a trusted source. The US and allied governments must establish a set of criteria to define what it means for a CIM manufacturer to be considered a trusted course.

How Chinese companies are "metastasising"

The section of the report below looks at how the two biggest Chinese CIM manufacturing companies, Quectel and Fibocom, have established or partnered in "non-Chinese" companies which play down or obscure their involvement in CIM supply. Why is this necessary if there is nothing to hide? The new companies discussed below are using established technology, not their own. It is not possible that they could suddenly emerge in the marketplace with their own intellectual property and know how, when established CIM suppliers have spent tens of millions of dollars annually over a decade or more in research and development. Moreover, given low margins in the CIM business, to make any profit and return on capital, these newly set up "non-Chinese" companies simply could not develop their own separate technology to compete with larger, established players in a meaningful timeframe.

This, then, is the main problem with the recently established companies considered below: their continued use of Chinese technology. Unless US and other governments put in place proper safeguards, the claims of these companies that in this age of geopolitical tensions they represent a trusted supply are without foundation.

- Netprisma and Wireless Mobility

Quectel set up NetPrisma in April 2023 as an American company based in Washington state.[10] Netprisma manufactured in Malaysia and, it claims, in the US. A job advertisement for its R&D base claimed that: "Netprisma Penang is the biggest R&D center around the world"[11] (this seems surprising given that the company in Malaysia was only incorporated in December 2024,[12] which also suggests that it was not doing its own research, but rather using Quectel's technology). Despite being an 'American' company, NetPrisma used Shanghai-based SGS-CSTC Standards Technical Services as its test/certification laboratory. While this does not prove that its technology is Quectel's or Chinese, it does raise questions of whether western governments should trust the certification, given the ability of the CCP to control all companies within China. It is noteworthy that several of NetPrisma's user manuals give a Quectel person as the contact for the manual.[13] Elsewhere, in a brochure description of another device, an engineer noted: "Netprisma: new plugin with support for Netprisma (ex-Quectel) devices", demonstrating an assumption that NetPrisma devices were "ex-Quectel".[14] The registered "governor" of NetPrisma is Qian Zekai (written as Zekai Qian).[15] The CEO of Quectel is Patrick Qian. Qian Zekai is said to be his son, although this has not been fully established.

[10] 'Quectel is attempting to defend its customer base by leveraging strategies such as launching the Net Prisma brand and the 'Made in US' campaign with Eagle Electronics in addition to more aggressive pricing'
https://www.counterpointresearch.com/en/insights/nam-cellular-iot-module-shipments-q3-2024
[11] https://my.joblum.com/job/quality-system-engineer/1901554
[12] https://businessreport.ctoscredit.com.my/oneoffreport_api/single-report/malaysia-company/1597029M/NETPRISMA-TECHNOLOGIES-PENANG-SDN-BHD-
[13] Eg. kingson zhang@QUECTEL COM User Manual NETPRISMA INC LCUK54WWDA 2BEY3LCUK54WWDA lcuk54wwda. See: https://device.report/netprisma
[14] https://wiki.linuxfromscratch.org/blfs/ticket/21227
[15] https://static.bizprofile.net/wa23/1/4/7/9/6/3/1479630.pdf

In June 2025 NetPrisma was taken over by Wireless Mobility Holding GmbH, which describes itself as a 100% German-owned company. A look at the personnel at Wireless Mobility confirms close links with Quectel. Of the five leaders listed on Wireless Mobility's website, four came directly from Quectel. Details of the actual shareholders—such as the names of its financial backers—are not publicly disclosed. However, on its website Wireless Mobility describes Quectel as an "affiliate" with which it may share data:

> "Depending on the subject of your inquiry, we may share the information you provided and your personal data with **our affiliated companies, in particular with Quectel Wireless Solutions** [*bolding added*] Co., Ltd. Building 5, Shanghai Business Park Phase III (Area B), No.1016 Tianlin Road, Minhang District, Shanghai 200233, China, if we consider that the affiliated company can better serve your request or for internal administrative purposes."[16]

Norbert Muhrer, until May 2025 President and Chief Sales Officer of Quectel and now CEO of Wireless Mobility, declared that, "According to third party analysis, the IoT market is void of a strong Western vendor, OEMs [Original Equipment Manufacturers] require choices to navigate the growing geopolitical and cybersecurity demands, and they need trusted partners who can offer both technological excellence and regional alignment."[17] While this statement cannot be faulted – Wireless Mobility is indeed a western vendor – the issue of trust depends crucially upon the source of the technology and the input into FOTA updates. If the technology and source codes are Quectel's and are controlled by Quectel, any firmware over the air (FOTA) updates would also originate from China and be a threat to security. "Manufacturing is carried out at EMS [electronic manufacturing services] partners in Malaysia and the US." It is not clear where in the US this manufacturing is carried out. Wireless Mobility needs to say precisely, so that the trustworthiness of the manufacturing facility can be assessed.

- Ikotek

Quectel also set up Ikotek, which offers design and manufacturing of IoT products.[18] According to Quectel, "Ikotek is an extension of Quectel's in-house engineering services to offer a full solution from design to manufacture."[19] Senior Ikotek figures have also openly described Quectel as Ikotek's "parent company". In press releases, Ikotek describes itself as 'a vital component of the Quectel family".[20] Their collaboration is close on product development and certification. Based in San Diego, Ikotek emphasises that it is an American company.[21] However, its technology is Chinese, and therein lies the problem.

- Quectel and Eagle Electronics

In 2024 Quectel entered a joint venture called Eagle Electronics, based in Ohio and set up with American money. It manufactures in Ohio. Its website states:

> "With full control over the entire manufacturing process, Eagle Electronics offers you an uninterrupted supply chain while fueling the American economy.
>
> We've partnered with Finite State, a leader in software and device security, to independently verify there are zero vulnerabilities in the source code, build process, and final binaries of all our devices.

[16] https://www.wirelessmobility.com/privacy-policy/
[17] https://www.germanyinthenews.com/article/818109582-wireless-mobility-and-netprisma-unite-under-new-ownership
[18] https://market.quectel.com/invitation/ces/2022/masterclass/index.html
[19] https://www.quectel.com/news-and-pr/quectel-sets-out-highlights-of-ces-2022-program/
[20] "Top IoT industry executive Mathi Gurusamy joins Ikotek as COO". https://www.businesswire.com/news/home/20231120698687/en/Top-IoT-industry-executive-Mathi-Gurusamy-joins-Ikotek-as-COO
[21] https://www.ikotek.com/company/about-ikotek/

> Leveraging our partnership with industry leader Quectel, we've capitalized on proven technologies and manufacturing processes that keep production costs down while engineering the best devices on the market."[22]

Manufacturing CIM hardware is not difficult. Eagle Electronics uses Quectel's source codes and technology in its products.[23] It is surprising that Quectel is prepared hand over control of the inner sanctuary of its technology, to NetPrisma/Wireless Mobility or Eagle Electronics (a parallel might be with Coca Cola, which licences production of its beverage, but never allows the secret of its recipe to leave its control). To be considered a trusted supplier, these new companies need to show that Quectel has indeed licensed to them the full source codes.

Quectel would surely be reluctant to hand over source codes. In 2020, China passed an Export Control Law. It applies to "the State's export control over dual-use items, military items, nuclear items and other goods, **technologies,** services and items relating to the maintenance of national security and national interests,…"[24] The law applies to civil use, as well as to military uses, the production of weapons etc. The bans apply for reasons which include harming the national interest. All this is line with CCP's policies aimed at dominating the IoT market, not least in CIMs.

Certification/verification of the CIM product is vital for the concept of being a trusted supplier. Not only the source codes, future technical developments, but also the regular firmware updating of the CIMs to patch glitches as they emerge must be examined to ensure their cleanliness. Throughout the life a CIM there must be a guarantee that Chinese companies do not have the ability to introduce malware. Eagle Electronics' partner Finite State claims that it verifies that there are "zero vulnerabilities in the source code". This is an ambitious statement. The US government needs to satisfy itself that it accords with reality and that Finite State has checked every line of code in the original product and in the updates.

'Who will guard the guards?' is a concern. Eagle Electronics and Finite State have a close cooperative connection. The founder and CEO of Finite State is a founding board member of Eagle Electronics.[25] There would also appear to be overlapping investment between the two companies: the Eagle Electronics founding investor group had earlier invested in Finite State.[26] This raises questions about the independence of any certification.

One requirement for security would be that Eagle Electronics and Wireless Mobility should have large banks of servers in the US and Europe for processing the firmware updates. The details of each individual CIM, its end user, deployment, IMEI number, location, environment, company, role, condition, phone numbers and carriers, and much more are known to its manufacturer. All this is necessary for performance monitoring and for firmware updates. Furthermore, tech companies need to back up their servers in other countries in case of emergencies (war, weather, earthquakes, civil strife etc), so that if, as happened in the attack on the World Trade Centre, a company loses all its data, it can be recovered without pause. This is known as 'mirroring', exact copies of the servers, kept in other countries. Thus, claims that there are "zero vulnerabilities in the source code" would not be reassuring if the country where a 'mirror' was located turned out to be China. All data would be in

[22] https://www.eagleelectronics.com/about-us/
[23] Eg. IATF 16949 – Automotive Grade 5G NR Module
"AG555Q-GL is one of the automotive-grade 5G NR Sub-6 GHz modules developed by Quectel, supporting both 5G NR NSA and SA modes."
https://www.eagleelectronics.com/products/a5555q/
[24] Translation of the Export Control Law is available at: https://www.chinalawtranslate.com/en/export-control/
[25] https://www.eagleelectronics.com/about-us/
[26] https://www.acp.vc/post/made-in-america-announcing-our-investment-in-eagle-electronics

China, useful if they wanted to 'kill' certain functions and services in the US. Companies need to show that they have no servers in China and that their servers elsewhere are not vulnerable to Chinese penetration.

Given the above and as a minimum for qualification as trusted suppliers, companies manufacturing outside China but using Chinese technology, need to be able to answer the following questions:

- Do they have full access to Chinese source codes?
- Can they show that their manufacturing processes are not vulnerable to Chinese interference?
- Do CIM manufacturers and certifying/verifying companies have sufficient staff to monitor all firmware updates?
- Are firmware updates connected *in any way* to servers in China?
- Do they have server capacity in the US or Europe, sufficient to service every CIM sold?
- In which countries are their primary servers located and in which are they mirrored?

For Eagle Electronics and Wireless Mobility to be able to claim that they are trusted suppliers which geopolitical needs, they must show that they can answer in detail and satisfactorily the questions above.

- Fibocom, Rolling Wireless and Europa Solare S.R.L.

This same process of setting up companies ostensibly unconnected with mainland Chinese entities appears to be what Fibocom, the second biggest Chinese CIM manufacturer, has done. In July 2020, Fibocom led a consortium which bought the Shenzhen-based automotive CIM manufacturing business of Sierra Wireless, a Canadian company. 49% of the new entity Rolling Wireless, headquartered in Luxembourg, was owned by Fibocom, with the remaining 51% owned by three leading investment firms based in China.[27] Just over two years later Fibocom bought out the investment firms and took full control of Rolling Wireless.[28] Then in July 2024 Fibocom sold Rolling Wireless to Europa Solare S.R.L., a Luxembourg-based fund backed by international investors from Europe, North America, and Asia, with the aim of "reinforcing its European identity".[29] This was "in response to complex changes in the current international market environment", a reference presumably to possible security measures to be taken to allay worries connected to Chinese technology.

The identity of the investors in Europa Solare is not publicly available. Fibocom declared that, "The company will continue to operate independently under the new ownership. There will be no changes to Rolling Wireless's management, locations, daily operations, strategic goals, or product strategy as a result of the ownership change."[30] While all that may be true, it does not cover the question of the threat from using Fibocom's technology, and thus avoid the danger of FOTA updates discussed in this paper. Indeed, the lack of change trumpeted suggests that the technology used by Europa Solare is from Fibocom.

For Europa Solare to fit the bill of being a trusted supplier, they need to answer the same five questions listed above in the instance of Eagle Electronics, to make clear who owns the company, and to be open about the source of the technology which they are using. In the absence of that information, the

[27] https://www.sierrawireless.com/company/newsroom/sierra-wireless-reaches-definitive-agreement-to-divest-automotive-embedded-module-product-line/
[28] https://www.fibocom.com/en/newscenter/fibocom-increases-investment-in-rolling-wireless,-which-remains-an-independent-operation.html
[29] https://www.rollingwireless.com/en/news/new-owner
[30] https://www.rollingwireless.com/en/news/new-owner

owners, whoever they might be, leave themselves open to the accusation that the setting up of Europa Solare was an instance of 'tech washing'.

Conclusion

Eagle Electronics, Wireless Mobility, Ikotek, and Rolling Wireless/Europa Solare all make much of the fact that they are non-Chinese companies, that they are "de-risk[ing] supply chains", and that, "Due to increasing geopolitical tensions coupled with cybersecurity concerns, …..there is significant demand for a new Western module provider."[31] There is indeed such a demand – or there should be, for national security reasons.

But these companies must be asked to demonstrate convincingly that they have sole charge of the sources codes they use, that their FOTA updates do not rely on Chinese engineers, servers and inputs, and that they do not have 'mirrors' based in China. In the absence of such proof, they cannot qualify as 'trusted sources' for CIMs.

Governments need to be clear that the importance of CIMs to national and economic security is on a level perhaps higher than that of rare earths. CIMs are crucial to the automotive industry, but also to nearly every aspect of the economy, be it routers, payment terminals, agricultural machinery, pipelines, manufacturing, logistics, telecommunications and in other critical national infrastructure. Ultimately, economic security and national security merge.

The concept of trusted supplier in the CIM context is vital. There should be no active Chinese technological input in trusted CIM sources. Chinese chipsets (eg. Huawei) are a well-known threat and have been widely blocked from western infrastructure. CIMs are 'chipsets through the backdoor', representing an effort to bypass restrictive measures on chipsets.

CIMs are not difficult to produce, production lines can be quickly set up. But reliable sources will only come to market if they have the finance. And the finance will only be forthcoming if investors can be confident that western companies will not be undercut by subsidised Chinese companies. The small extra cost of a CIM purchased from a reliable company is a small price to pay for national security.

Recommendations

Three years ago, there was little discussion of the threat from CIMs. Governments were more concerned with the export or theft of technology and intellectual property (IP), than with the dangers of importing components which use Chinese technology. That is changing. In the UK, after initial reluctance and some persuasion, the previous government created a "debarment list" in the 2023 Procurement Act. Companies listed on national security grounds are to be excluded from participation in government procurement contracts. The recently established National Security Unit for Procurement has yet to populate the list.

In the United States (US), Quectel, a company which ought to be as well-known in democracies as Huawei or Hikvision, has been put on the 1260H list.[32] Although this does not ban Quectel from operating in the US, it does raise red flags, and may be a harbinger of more restrictive measures in future. Department of Commerce's Bureau of Industry and Security (BIS) rule on connected vehicles

[31] "Wireless Mobility and NetPrisma unite under new ownership", https://www.wirelessmobility.com/wireless-mobility-and-netprisma-unite-under-new-ownership/

[32] For an account of the significance of the 1260H list, see: https://www.hoganlovells.com/en/publications/us-department-of-defense-issues-updated-section-1260h-chinese-military-companies-list-

and related hardware/software linked to China or Russia sets a model for other industrial sectors. The House Select Committee on Strategic Competition between the United States and the Chinese Communist Party has rightly taken an interest in the threat from Chinese CIMs, as has the Federal Communications Commission.[33]

Vehicles are crucial to a country's economic and national security. But if China's plans to attain a monopoly of the supply of CIMs succeed, **the three threats of dependency, disruption/destruction and data egress will apply not just to transport, but to almost every sector of national security, the economy and everyday life.** Therefore, it is important that free and open countries take comprehensive measures to prevent Chinese companies and the use of their technologies from getting round measures designed to mitigate these threats.

There remain trusted, non-Chinese CIM manufacturers, which do not rely on Chinese technology. These could easily increase production, given that CIM technology is not especially sophisticated. But time is running out: the Chinese intention to throttle them is proving effective in the absence of defensive measures.

Sadly, Chinese CIMs are already too endemic to allow wholesale 'rip and replace', whether in the vehicle industry or in wider systems. These components are buried in units in sub-systems in systems. Nevertheless, an exception must be made in the case of sensitive military and intelligence systems, and of the most critical of critical national infrastructure. The following measures should be researched and implemented as soon as possible:

- Conduct an audit of military, intelligence and the most sensitive critical national infrastructure to understand where Chinese CIMs pose a threat; replace these CIMs with those from trusted sources.

- Free and open countries should ban Chinese vehicle manufacturers from their markets (the US has done this; European and other allied countries have not).

- They should ban the use of Chinese CIMs or of CIMs using Chinese technology and algorithms in non-Chinese vehicles (in hand in the US) and in broader critical national infrastructure (still to be considered).

- Until the time when Chinese CIMs and Chinese algorithms are completely absent from vehicles, vehicles containing Chinese CIMs should be banned from sensitive military, intelligence and critical national infrastructure sites (as the Chinese have, rightly, done in the case of Tesla cars, fearing the transmission of sensitive data).

- Establish the concept of trusted sources for CIMs. American and European companies need to show that:

[33] In August 2023, the Select Committee wrote to the FCC, asking about measures concerning CIMs. The FCC in turn wrote to eight government agencies requesting information about the threat.

- Their technology and FOTA updates are not reliant in any continuing way on Chinese source codes or servers.

- Their manufacturing processes are not vulnerable to Chinese interference

- They and certifying/verifying companies have the staff sufficient in number and technological competence to produce and monitor all FOTA updates.

- They and the companies which certify their CIMs have server capacity in the US or Europe, sufficient to service every CIM sold.

- Their primary and 'mirror' servers are located outside China and where they are not vulnerable to Chinese penetration.

- Strictly implement the connected vehicle rule to ensure that companies from allied countries which export vehicles to the US abide by the restrictions set out above.

- In the wider context, apply similar restrictions to other elements of critical national infrastructure.

Such measures would encourage the finance to back trusted suppliers, because it would prevent geopolitically motivated undercutting by subsidised Chinese competitors. Not taking action is creating a threat which is worse than 'Rare Earths 2.0'. Have we not already learned that lesson?

About the author
Charles Parton has spent 30 of the last 44 years working on or in China, as a diplomat and as an associate fellow at three think tanks, the Council on Geostrategy, the Royal United Services Institute and MERICS. His work centres on the internal politics of China, and increasingly on the CCP's use of science and technology as a geopolitical instrument. In particular, he has focussed on cellular (IoT) modules, the CCP's intention to gain a monopoly of this vital component, and the threats which this represents to free and open countries.