COALITION ON
SECURE TECHNOLOGY
THE CELLULAR IOT MODULE THREAT

The Infrastructure Threat from Chinese Cellular (IoT) Modules (CIMs)

Charles Parton

This short paper aims to be a ready reference on the threat posed by the Chinese Communist Party's (CCP) plans to establish a monopoly of the supply of CIMs, crucial components in the Internet of Things (IoT) age.

What is a CIM?

CIMs are electronic wireless components embedded within units or systems. They contain software processing units, geolocation capability, e-sims to connect to the internet, memory, and other peripheral components. They transmit, receive and process data about their environments, independently of human action (hence IoT). They monitor and control complex systems remotely; ensure that such systems run efficiently; collect huge amounts of data and metadata for analysis, processing, and response management; and deliver software/firmware updates to improve functionality.

Why are CIMs important?

In effect, CIMs are the gateway to computers and the cloud, which today are integral to most systems. They are in our homes, in smart meters, security systems, home appliances, electronic payment infrastructure; they control modern cars; they are vital to industry, logistics, agriculture and transportation; they are integral to critical national infrastructure (CNI), such as pipelines, power grids, water supplies, and ports. By 2025 there will be around 31 billion worldwide, a number rising exponentially.

What is the current state of the global market?

Chinese companies such as Quectel, Fibocom, China Mobile, Sunsea, MeiG – names which should be as well-known as Huawei, Hikvision, or DJI drones, but are not – have over 70% of the global market, including over 80% in India. US, Canadian, Swiss, Japanese and Korean companies struggle to compete against heavily subsidised Chinese competition, which enjoys a protected domestic market.

What are Chinese intentions?

The CCP has designated CIMs as a key industry. Its aim is to gain a Chinese monopoly of supply, helped by providing favourable regulatory treatment, finance at preferential rates, access to land, key materials and products (such as semiconductors) at below cost, and other state support. This underwrites aggressive pricing by Chinese companies, often at between 15-25% below the costs of manufacture. Distressed foreign companies become targets for a Chinese take-over (in 2023, Fibocom bought Luxembourg-based Rolling Wireless).

What is the threat?

Chinese companies have no choice but to obey CCP instructions, not least national security laws, which bind them to obeying the authorities. Whether private or state-owned, companies must acknowledge – in Xi Jinping's words – that 'East, west, south, north, the Party leads all'. If Chinese CIM manufacturers gain a monopoly of supply, free and open countries would face three threats:

1. Dependency. The CCP could put pressure, directly or indirectly through companies, on governments to change policies – in any field – by threatening to withhold CIMs. Governments recognise the threat of dependencies in critical minerals; they are less awake to dependencies on vital components.
2. Degradation or destruction of systems, CNI, economic entities. CIM manufacturers develop software in CIMs, which could embed malware. They also send regular firmware updates over the air (FOTA).
3. Data and meta-data acquisition by the CCP on a massive scale. This could be focussed on an important individual, on a company, on government or on society at large.

How might such threats be weaponised?

The CCP is not yet in a position to exploit a monopoly over CIMs, nor, even if it had one, would it be likely in the near future to degrade or destroy systems in other countries. However, responsible governments must plan for the possibility of high tensions or even hostilities with China in the longer term. Potential flashpoints are already evident (Taiwan or the South China Sea), and China has been caught scoping out American CNI. Examples of what Chinese companies could do, if they had a monopoly – or even with a high market share – include:

- A 'high voltage' attack via smart meters to knock out the electricity grid, potentially for over six months ;
- Bring ports to a standstill by immobilising cranes (hence recent US worries about ZPMC cranes);
- Immobilise lorries belonging to defence forces to prevent military deployments (as John Deere did remotely through the CIM to agricultural machinery stolen by Russia from Ukraine. But it does not have to be the operator. The CIM manufacturer could also immobilise vehicles.);
- Obtain data from phones synchronised with car infotainment centres (the British security services discovered that data from the Prime Minister's car was being sent to China via a Chinese CIM);
- Obtain speech and films from inside private cars (Tesla engineers were sacked for doing precisely this);
- Access data passing through routers; or prevent routers from working to paralyse communications;
- Paralyse financial payment systems to cause economic and social chaos.

What should free and open countries do to counter the threat?

In most fields, 'Rip and replace' would be too expensive an option. The implementation of measures below would gradually meet the threat by imposing on Chinese companies restrictions similar to those imposed on foreign companies in China.

- Carry out an audit of Chinese CIMs in CNI, defence and security;
- Carry out research on the threat; and on the mutation of Chinese companies as they set up alternate entities (for example, Quectel has set up Ikotek for design, and Netprisma for manufacture. Although these are registered American companies and manufacturing is not in China, they are wholly Chinese owned, the software is Chinese and the threat in no way reduced);
- Establish a centre of government expertise to advise all departments, help with security plans and provide awareness training;
- Legislate and implement laws to exclude Chinese CIMs from all government procurement;
- Ban government departments from using vehicles with Chinese CIMs and prohibit private vehicles with Chinese CIMs from entering military and sensitive areas (car cameras are capable of facial recognition;
- Consider excluding Chinese CIMs from health services' equipment and systems (to comply with data protection requirements);
- Exclude Chinese CIMs from consumer telecommunications products such as routers;
- Legislate to ban Chinese CIMs in all CNI (under an updated definition of CNI);
- Provide support to maintain and increase the number of trusted suppliers/manufacturers of CIMs;
- Free and open countries should work together to agree on and to promote trusted suppliers.

Why is action easier than for some other technologies?

The concept of trusted suppliers is key.CIMs are not especially hi-tech components. If Chinese CIMs are phased out, existing non-Chinese suppliers could quickly ramp up production. Alternatively, governments could set up their own indigenous CIM industries.

Politicians can be assured that dealing with the threat of Chinese CIMs is considerably less complicated than the semiconductor question. Taking measures is a relatively easy political win.

Longer papers on CIMs are available at:
Chinese cellular (IoT) modules: Countering the threat
Cellular IoT modules – Supply Chain Security