Coalition on Secure Technology
The Cellular IoT Module Threat

Report by Charles Parton

Cellular IoT modules are at the heart of the 'Smart' technology we increasingly rely on. They are in our cars, our doorbell cameras, our metering systems, yet few of us are aware of their presence let alone the risks associated with their use. The Coalition on Secure Technology wants to change all that.

Our campaign aims to raise awareness of the threat potentially posed by the use of these components to our national security, to our economic prosperity and to our privacy. We want to highlight the need to avoid economic dependency for this technology on countries which do not share our values.

More than half of the international market in Cellular IoT modules (CIMs) is already in the hands of five Chinese companies, yet these devices can share our data, they control parts of our critical national infrastructure, and they can be accessed remotely. Those of us who live in free and open countries need to consider how this might be a danger.

The United Kingdom's protracted policy debate over Huawei and 5G telecommunications was a wake-up call. Since then, the government has tended to play 'whac-a-mole', taking aim at companies such as Hikvision or Dahua, rather than looking at generic threats. The greatest threat comes from cellular internet of things (IoT) modules and the Chinese Communist Party's (CCP) intention to ensure that Chinese companies, which must obey its diktats whatever their ownership structure, dominate and eventually monopolise their supply.

What is a cellular IoT module?

Cellular Modules are electronic components embedded in larger devices or sub-units rather than finished items, such as CCTV cameras or drones. They connect to the internet, via an 'e-sim', just as a mobile phone does. They enable devices to be connected externally to other devices or systems, or to an internal server.

Cellular modules are not semi-conductors or simcards, although they contain both. They have processor units for power, modem and applications, filters, amplifiers, antennae and memory. They are not necessarily hi-tech, although with the spread of 'edge-computing' they are increasingly able to do tasks previously carried out away from the systems to which they are linked.

Industries, agriculture, critical national infrastructure (CNI), 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. They are, in effect, communication computers, the gateway to systems. Without cellular modules we would not have 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.

Trusting your cellular module

Module manufacturers leverage economies of scale to source components and offer a packaged solution. Installing a company's modules requires the user to be able to trust the manufacturer, particularly their firmware. Not only has the manufacturer written in large amounts of code to start with, but cellular modules must also include the ability to update software remotely. This is essential

for fixing problems, enhancing performance, adjusting to mobile network operator settings, or implementing security patches. The role of the module manufacturer goes beyond merely supplying the component; it extends to supporting customers in keeping their equipment up-to-date and secure.

This is a lifelong umbilical cord. It gives manufacturers significant insights into their customers' equipment and processes. Users must also be confident that nothing malicious will be installed in the numerous updates; yet it would not be possible to check every individual update throughout the life of the module.

"Trust me," said the crocodile to the monkey……

Customers using Chinese cellular modules are in effect putting their trust in the CCP, because by law and by the realities of CCP power no Chinese company can ignore the Party's orders to help in national security matters – which the CCP itself defines, often ad hoc.

The IoT is one of the areas of new technology which the CCP is targeting for domination. Currently its companies have secured around 64% of the global market (the leaders are Quectel 38.9%, Fibocom 8.7%, and MeiG 5.6%, while the biggest non-Chinese company is Telit/Cinterion 8.6%). 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. The intention is to drive out foreign competition, including through underhand targeting of competitors' main clients.

The threat from Chinese cellular modules

If the CCP attains its objectives for Quectel and other cellular module national champions,[1] it will attain considerable powers over free and open countries, namely:

1. Access to very large amounts of data.
2. The ability to put pressure on foreign companies, organisations and governments by using the threat to withhold supplies.
3. Establish a dependence on the part of foreign countries on Chinese suppliers for the continued operating and functioning of their CNI.

The common reaction to these threats is, where is the evidence, the smoking gun? A trite answer would be that if governments and agencies have not been aware of the problem of cellular modules, then they have not even been looking for the evidence. More seriously, it is the business of a responsible government to anticipate, to defend against threats in advance of their breaking. No one goes into a boxing ring, gets beaten up and only then decides that they had better learn how to box and get fit. Or to put it another way, which would you rather face: a smoking gun or a loaded gun?

The CCP sees itself in an existential struggle with America and its allies, its intentions – by its own declaration – are hostile.[2] Threat is a combination of hostility, intention and capability. It is that capability which responsible government must guard against – in the worst case, at a time of tension or conflict, the CCP could degrade or halt the operations of our CNI.

[1] For a detailed look at the CCP's policy on cellular modules, see Charles Parton, "Cellular IoT modules – Supply chain security" https://www.oodaloop.com/wp-content/uploads/2023/02/Cellular_IoT_Paper_JAN_Master_PDF.pdf),

[2] See Charles Parton, the Council on Geostrategy, "Is China a threat?", which uses the CCP's own words to elucidate the threat. https://www.geostrategy.org.uk/research/is-china-a-threat/

And we are handing that capability to the CCP. To take the three threats listed. Firstly, data. Back in January an iNews report talked of a government car being taken apart by security officials because data could be sent back to China through the "e-sim", i.e., the cellular module.[3] One very senior government source separately said that the government was petrified by the problem. This incident should be no great surprise, because earlier Tesla engineers had been sacked after they had listened to conversations and watched films taken remotely from Tesla cars – via the cellular module.

Secondly, pressure to change policies. Experience during the Covid pandemic and threats to withhold supplies of PPE, as well as broader dealings with the CCP, has shown that for the Party there are no boundaries between commerce and geopolitics. If Quectel, Fibocom and others gain a monopoly on supply, UK government policies could be held to ransom.

Thirdly, threats to shut down CNI. This is not fiction. When Russia stole from Ukraine large quantities of John Deere agricultural machinery, via the cellular modules John Deere simply turned it all off, reducing it to useless lumps of metal. To take other examples. Smart meters in your home might appear innocent enough, and they have important functions in terms of ensuring efficient operation of the grid, thereby helping to reduce environmental concerns. But with a Chinese monopoly on supply, covert software instructions could be used to unbalance and bring down the grid. Or how about stopping all government (and private) cars and transport?

Wake up

The CCP itself understands and takes the problems seriously. It does not, for example, allow Tesla cars in the vicinity of the Party leaders' summer retreat at Beidaihe, and it banned them from Chengdu when Xi Jinping recently visited there. In November 2022 Quectel issued a "Product Change Notification", detailing a new firmware upgrade which prevented modules from working in Russia or Iran. Although this move was in support of embargos, it demonstrates how firmware updates can disable module functionality. If there, why not in the UK?

The UK government is waking up to the problem of cellular modules. After representations were made, it has amended the Procurement Bill so that no Chinese company subject to that nation's security laws can be in the supply chain of those bidding for government contracts. This is an important start, although it remains to be seen how rigorously the law, when passed, is implemented.

Surprisingly, for all its measures on technology the US has been slower off the mark. Awareness is rising: recently the House Select Committee on China wrote to the Federal Communications Commission seeking clarification on its views on Chinese cellular modules. Late in the day, but perhaps there will be action at the federal level. That may take time to percolate down to state level.

Sadly, there is no evidence that the European Union has even considered the problem, and in India, which banned TikTok, market penetration by Chinese cellular module manufacturers has reached 86%.

The remit of the Coalition on Secure Technology

In sum, a monopoly of the supply of cellular modules would give the CCP immense power, even to win a war without fighting. Free and open countries have been asleep at the wheel. This is not about being anti-China, but about protecting our CNI and our future. Sadly, we have entered a different world, one where the distinction between civil and military technology is fast eroding and one where "techno-repression", championed by the CCP, is advancing at pace. While we should preserve as much

[3] https://inews.co.uk/news/hidden-chinese-tracking-device-government-car-national-security-2070152

cooperation and interaction with China as possible, we must not help give further substance to the threats of a power which declares itself hostile to us. China has long been clear eyed about pursuing and protecting its own interests. We should be the same.

Our purpose is to raise awareness of the risks associated with the use of Cellular IoT modules whose provenance could be a threat to our security, our prosperity, our privacy and our human rights.