Cellular IoT modules – Supply Chain Security

by Charles Parton

Acknowledgement: Significant technical expertise has been provided by Dr Samantha Hoffman

WHAT IS THE CONCERN?

Free and open nations have woken up to the threat posed by Chinese involvement in their 5G telecommunications and to the importance of maintaining the lead in semiconductors. There is less awareness of the risks incurred by using Chinese cellular IoT technology. In the longer term the risk posed by the pervasive presence of Chinese cellular IoT modules in our systems and processes poses a greater threat than does relying upon Chinese companies for 5G.

Three Chinese companies already have over 50% of the international market for cellular IoT modules (since that includes the large Chinese domestic market, the percentage, while worrying, do not represent a lost cause). Their products are found in a huge range of applications. CCP policy documents show the strategic importance of IoT technology to the Party. In line with CCP industrial policy to promote global champions in new industries, IoT companies have benefited from the creation of a domestic market which excludes international competition, sets preferential pricing regimes, and provides access to subsidies and centralised funding.

The risk is that, if Chinese companies continue to increase global market share and to edge out foreign companies, free and open countries will become dependent upon China for cellular IoT modules. Given the immense importance of these modules to modern industry and life, this would make other countries highly vulnerable to a threat to withhold supplies. Dependency is dangerous when it is in the hands of the CCP, a potential, if not actual, hostile power.

More specifically the threat revolves around four areas: national security, economic prosperity, privacy, and values and human rights. Concerns include:

- Degrading the performance or even sabotaging critical national infrastructure and key industries
- Losing sovereign control over IoT and over capabilities in dependent technologies/industries
- Unfair economic competition leading to the loss of domestic IoT industry
- Losing sovereign control of strategic data
- Enabling more espionage and theft of intellectual property
- Sustained collection and misuse of personal information without consent
- The potential for CCP security organisations to carry out detailed surveillance from within our societies (eg in smart cities)
- The expansion and support of technological capabilities applied in human rights abuses in Xinjiang, wider China, and increasingly in third countries

This vulnerability and threat are real and current. In January 2023, the UK media reported that a surreptitious Chinese cellular IoT module had been discovered in UK government cars, including those used by senior government minsters. The module, which was described as a "tracking device" was reportedly identified after officials had dismantled the British Government vehicles and swept them deliberately for what it referred to as Chinese "tracking" devices. Quoting serving intelligence sources, the media reported that the devices had been concealed inside sealed parts from suppliers in China.

WHAT IS THE SOLUTION?

The longer the delay in limiting Chinese IoT modules, the more difficult and expensive it becomes to phase them out. Absence of action will lead to a dangerous dependency on the CCP, which will be able to put pressure on foreign policy makers by threatening supplies.

As ever, science moves with lightning speed, governments more glacially. Nevertheless, it is time to wake up. In one sense, recommendations can be reduced to one simple imperative: Free and open countries should ban Chinese manufactured IoT modules from their supply chains as soon as possible

More realistically, they should:

1) Push forward more quickly their research into the issue of cellular IoT modules and broaden understanding of its implications for security, economic prosperity, privacy and values.

2) Develop training to make all government departments aware of digital supply chain risks, particularly in the IoT sector.

3) Conduct a thorough audit of where these Chinese modules are embedded in government properties and services, and in critical national infrastructure, in order to measure the extent of potential risk and to prioritise areas for remedial action.

4) Require government departments to produce plans to mitigate the risks identified in their areas.

5) Pass legislation or implement administrative measures to prevent the purchase of new Chinese IoT modules for domestic manufacturing and services, with a deadline of the end of 2023.

6) Since the immediate replacement of Chinese modules in existing products and services is not practical on expense grounds, governments should allow a grace period of reasonable length, during which companies operating in sensitive areas are required to replace already installed Chinese modules, perhaps by the end of 2025.

THE INTERNET OF THINGS (IoT) AND CELLULAR MODULES – THE NEW SECURITY AND COMMERCIAL FRONTIER

The Internet of Things (IoT) is fast becoming the central nervous system of the global economy. The IoT spans energy, supply chains, manufacturing, agriculture, transport, urban planning, security, domestic applications, and increasingly all aspects of the human-to-machine and machine-to-machine interface.

The embedded sensors, software, processors, communication hardware and other technologies collect, send and act on data they acquire from their environments. They connect and exchange data with other devices and systems over the internet without human intervention, forming an

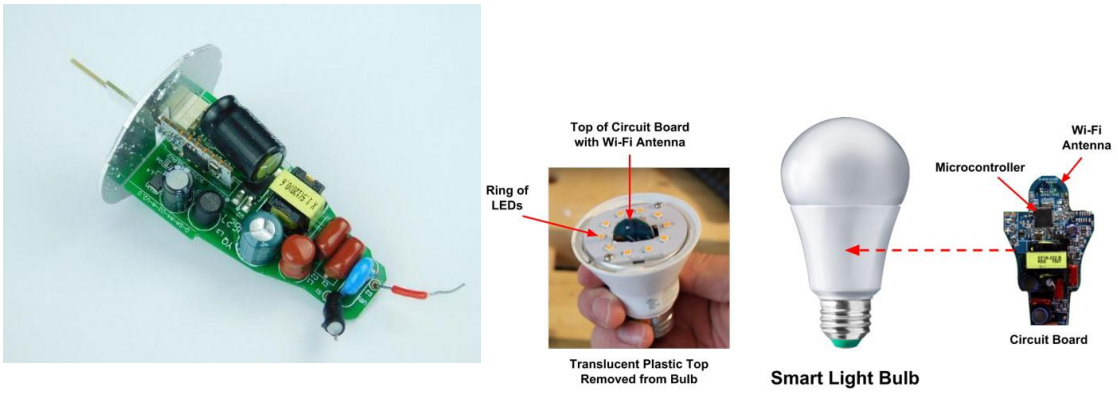
IoT ecosystem. This data is collated and transferred to back-end systems for analysis and action. Using artificial intelligence (AI) and machine learning can make data collecting and processing easier and more dynamic. IoT modules are used in environments ranging from ordinary household objects to sophisticated industrial tools and processes.

This enabling technology serves as a foundation for a wide number of downstream capabilities across an array of cutting edge and emerging technologies including artificial intelligence, machine learning and analytics, green energy, space, and robotics. IoT devices feature in manufacturing, logistics and utility organisations, as well as in defence, security, agriculture, infrastructure, home automation, amongst many other applications.

The Internet of Things (IoT) encompasses a wide range of products and dependent services which increasingly play a prominent role in key industrial sectors, infrastructure projects, and in the day-to-day lives of people all over the world. Common IoT devices, which might be seen in businesses and homes, include smart speakers, smart thermostats, smart security systems, mobile point of sale devices, medical monitoring devices, watches and other wearable devices, to name just a handful. An IoT network describes smart environments, like a "smart home", "smart industry" or "smart city". IoT applications in business includes things like supply chain management, and in government includes the provision of streamlined public services.

Most IoT device users only see a product's user interface. A simple example of an IoT device many people may have come across personally is a smart light bulb, like the Philips Hue. Instead of being controlled by a light switch, they can be controlled by mobile application, like the Phillips Hue app or by voice through another commonly used IoT device, a smart speaker, like Amazon Alexa or Google Home. A smart lightbulb combines energy-efficient LED technology (i.e. light-emitting diodes, a semiconductor device[1]) and a physical module that enables its communication with the applications and devices used to control it.[2] The images in Figure 1 are of what a module on printed circuit board in an IoT Device looks like in the example of a smart lightbulb.

Figure 1: What Makes a Device "Smart"?



Source: "Teardown: Hive Smart Bulb", All About Circuits, online (left) and "Smart Light Device", Code: Internet of Things, online (right).

[1] https://byjus.com/physics/light-emitting-diode/

[2] https://www.fluxsmartlighting.com/blogs/news/the-anatomy-of-a-smart-bulb-what-makes-them-so-special or https://www.allaboutcircuits.com/news/teardown-tuesday-wifi-connected-led-bulb/

IoT modules run their own operating system to interface with the host machine or appliance. The physical module is the key component of all IoT devices, it is typically assembled on a printed circuit board (PCB). There are several types of wireless technology used in an IoT module. IoT modules range in complexity from early-technology 2G and WiFi modules through to more advanced standards, such as 5G, 4G and LTE.[3] In the smart lightbulb example above, the module is relatively simple – depending on type and how it runs, it will use Z-Wave, Zigbee, Wifi and/or Bluetooth capabilities to communicate.[4]

Cellular IoT modules fulfill a critical role as part of IoT systems or products in serving as the gateway for data transfer through 5G, 4G, and LTE. They are responsible for ensuring the connectivity of the devices to which they are attached. They enable IoT devices to connect to each other within an internal network, and to connect externally with services, devices, or systems outside the network in which they are physically present. Their use is predominantly found in settings where other forms of connectivity are unsuitable, or where loss of connectivity would result in critical failure of systems. They also serve as back-up in systems which cannot afford to lose connectivity. They are often deployed in industrial settings that are part of critical national infrastructure including energy, transportation, communications, and finance.

Cellular IoT modules therefore often act as a single point of entry and exit for vital flows of data for the monitoring or control of systems that are critically important for the social, economic, and physical wellbeing of individuals, companies, and nation states.

Figure 2: Cellular IoT Module.

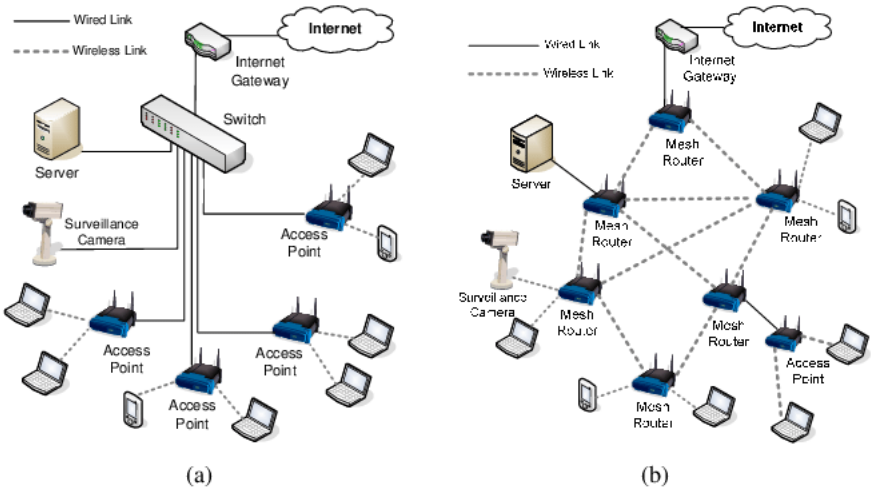
Source: Quectel Narrowband-IoT module, Quectel, online.

Cellular IoT modules combine radio transceiver, antennae, satellite positioning, baseband, applications processor and PMU, all integrated onto a printed circuit board less than 5x5 centimetres in size. This created microprocessor is always connected to the internet. These devices will be capable of constructing their own "mesh network" (that is a network of IoT devices

[3] Long Term Evolution, a wireless communication standard that bridged the gap between 3G and 4G
[4] https://www.smarthome.com.au/how-does-smart-lighting-work/

or ‘nodes’, where each node is connected to all other nodes in the network). A mesh network acts as an independent component capable of collecting, processing, sending, and receiving data.

Figure 3: Traditional WLAN versus Wireless Mesh Network



Source: Marius Portmann, *‘Wireless Mesh Networks for Public Safety and Disaster Recovery Applications’, Scientific Figure on ResearchGate. Available online.*

These modules will form the backbone of future mesh networking technology where devices form an overlapping and non-hierarchical connectivity. Such an arrangement is more resilient and offers far greater coverage than alternatives. Cellular IoT modules are increasingly commonplace within large scale infrastructure projects and critical national infrastructure. These devices harvest and transfer vast amounts of data in their day-to-day operation. Should this data be misused it could provide a highly detailed picture of the systems in which they operate, the individuals which come into contact with them, and the services that they support. Misuse of this data and the ‘pattern of life’ analysis which could be created from it, for example drawing on ‘smart’ cities and connected industries, could harm national security and individual safety.

WHY THE CCP WISHES TO DOMINATE THE MARKET FOR CELLULAR IoT MODULES

The Chinese Communist Party’s long-term strategy is set out in its ‘Two Centenary Goals ’(两个一百年). The first was to reach a “moderately prosperous society”, whose achievement Xi Jinping declared in 2021, marking the 100th year since the founding of the Chinese Communist Party.[5] The second, the “Chinese Dream” (中国梦) of the “great national rejuvenation of the Chinese nation” (中华民族的伟大复兴) is due by 2049 – the year of the 100th anniversary of the establishment of the People’s Republic of China (PRC).[6]

[5] ‘Xi Focus: Leading China on its new journey,’ Xinhua, 1 October 2021, online; ‘ [实现中华民族伟大复兴中国梦的关键一步]’, People’s Daily, 3 July 2021, online; ‘[习近平代表党和人民庄严宣告，经过全党全国各族人民持续奋斗，我们实现了第一个百年奋斗目标]’, Xinhua, 1 July 2021, online.

[6] The two centennial goals as laid out in the report of General Secretary Hu Jintao at the 18th Party Congress in November 2012: “只要我们胸怀理想、坚定信念，不动摇、不懈怠、不折腾，顽强奋斗、艰苦奋斗、不懈奋斗，就一定能在中国共产党成立一百年时全面建成小康社会，就一定能在新中国成立一百年时建成富强民主文明和谐的社会主义现代化国家” https://www.mfa.gov.cn/ce/cezanew//chn/zt/18da/t988429.htm

The language of national rejuvenation centres on making China a 'strong, democratic, civilized, harmonious, and modern socialist country'. This requires more than domestically-oriented success. It creates considerable challenges for China's strategic competitors, because ultimately its achievement translates into an intention on the part of the CCP to supplant the United States as the world's leading superpower, and to re-align the existing global order in such a way that it buttresses the interests and values of the CCP's system of authoritarian governance.[7]

New and emerging technology is central to the CCP's ability to achieve these goals. This is not just a question of possessing technical capabilities which promote economic development or military might, nor of spreading globally the surveillance and other illiberal applications of technology which the Party has implemented domestically. The most game-changing advantage of technology is that it enables the accumulation of massive amounts of data. The CCP views data as a strategic resource.[8] When processed and aggregated, data can support its interests across military, economic, political, cultural and other domains.

Internet of Things technology, or IoT technology, is a specific sector of concern.[9] IoT describes physical objects "embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet."[10] The specific technology enabling IoT, and the focus of this report, are IoT modules, especially the 5G related Narrowband IoT (NB-IoT) modules, a cellular radio access technology.[11] IoT modules are the mechanism by which data is transmitted and received by an IoT device, so they are the key component that make devices 'smart'. As a topic for policy discussion, IoT modules probably go under the radar because it is it is an internal component part which users do not tend to see when interacting with an IoT device.

China's domination of the global IoT market creates an opportunity for significant data collection and sharing. The risks China creates in the IoT sector are vast. As pointed out in a 2021 report by the highly respected Australian Strategic Policy Institute (ASPI) entitled *Mapping China's Technology Giants: Supply Chains and the Global Data Ecosystem*[12], suppliers to the companies which provide IoT devices can obtain downstream data access, and, regardless of a device's end-use, process that data for other uses. In the case where Chinese companies are the suppliers, this might undermine the interests of the individuals whose data has been collected. It could also be deleterious to the interests of nations in a strategic competition with China. Likewise, its 2019 report *Engineering Global Consent* described a specific case study relating to smart cities where IoT technology, among other things, was facilitating data collection which supported China's state security efforts, including in the fields of propaganda and intelligence.[13]

---

[7] See Daniel Tobin, Hearing on a 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards: How Xi Jinping's 'New Era' Should Have Ended U.S. Debate on Beijing's Ambitions. (2020), online.

[8] Eds. Emily de La Bruyère, Doug Strub, and Jonathon Marek, "China's Digital Ambitions: A Global Strategy to Supplant the Liberal Order, " National Bureau of Asian Research, NBR Special Report No 97, 1 March 2022, online.

[9] Alexi Drew, "Chinese technology in the 'Internet of Things' poses a new threat to the west", *Financial Times*, 10 August 2022, online.

[10] https://www.oracle.com/au/internet-of-things/what-is-iot/

[11] https://www.gsma.com/iot/resources/nbiot-deployment-guide-v3/

[12] Hoffman, Samantha, and Nathan Attrill. Mapping China's Technology Giants: Supply Chains and the Global Data Collection Ecosystem. Australian Strategic Policy Institute (8 June 2021), online.

[13] Hoffman, Samantha. Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion. Australian Strategic Policy Institute (2019), online.

State support for IoT[14] and cellular IoT module development in China has been significant. Specific to IoT modules, in 2017, the MIIT issued a Notice on Comprehensively Advancing NB-IoT Development, calling for the expansion of NB-IoT use in smart cities and industry, and in the home. It also called for support of companies producing NB-IoT modules and an acceleration of R&D related to NB-IoT modules.[15] Chinese companies now account for over 50% of global shipments of IoT modules,[16] and as of late 2020, accounted for 75 percent of cellular IoT connections worldwide. Quectel and Fibocom are the two largest players in the Global IoT market, accounting for just under 47 percent of market share in terms of IoT module shipments. By 2023 they may lead in 5G connections.

The implications of China's dominance of the global cellular IoT market have not yet been widely recognised.[17] At the very least, risk emanates from China's state security laws and the realities of everyday existence, all Chinese companies, whatever their ownership structure, have no choice but to heed the orders of the CCP. And as General Secretary Xi Jinping assures us, the CCP "leads everything". If the CCP wishes these companies to exploit these devices to interrupt or degrade critical infrastructure systems, or to hand over vast quantities of personal, industrial data, and national security data, they have no choice but to obey.[18]

In the CCP's quest to achieve national rejuvenation – or to speak bluntly, to become the number one superpower – given its ever increasing and extensive presence throughout industry and people's personal lives, cellular IoT modules could play an important role. Free and open countries need to recognise this challenge and must raise their defences accordingly.

HOW THE CCP SUPPORTS THE CHINESE CELLULAR IoT MODULE SECTOR

In the IoT sector, the party-state ensures that IoT companies receive favourable regulatory treatment, finance at preferential rates through central and regional banking institutions, access

[14] 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 (MIIT) referred to the IoT as a "strategic high ground". In the 13th Five Year Plan, which covered 2016-20, the section on digital and telecoms 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 Initiative (BRI). 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: https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf; https://merics.org/en/report/connection-everything-china-and-internet-things. The IoT also appears frequently in the 13th Five Year Plan. In special column 9, it talks of '2. Expansion of the internet of things: We will establish infrastructure for application of the internet of things and service platforms, and promote the creation of important demonstration projects for the application of the internet of things. We will broadly develop the integrated application of the internet of things as well as development of innovative models, and enrich services related to the internet of things.'

[15] https://archive.ph/Xo2vd

[16] https://www.counterpointresearch.com/global-cellular-iot-module-shipments-q2-2022/

[17] Though some have flagged the risk, for example: https://www.counterpointresearch.com/quectel-widens-gap-with-competition-in-global-cellular-iot-module-market-during-q2-2020/ and Greg Levesque chapter in https://www.nbr.org/wp-content/uploads/pdfs/publications/sr97_chinas_digital_ambitions_mar2022.pdf

[18] '中华人民共和国国家安全法' [State Security Law of the People's Republic of China], Gov.cn, 1 July 2015, online.

See articles 11, 77-79./

to key materials and products (such as semiconductors) at below cost, and other state support. These measures create a favourable and interconnected ecosystem for technology companies working on these strategic technologies.[19]

This matches CCP efforts seen in other sectors, such as telecoms, solar photovoltaic (PV) manufacturing, and high-speed rail. Using massive industrial subsidies, restricted government procurement policies, land grants at very low cost, IP theft and other levers, the CCP has built up new industries and pushed foreign competitors out of its markets – and often into bankruptcy. The next step has been to overwhelm competitors in the global market by subsidising expansion, giving cheap loans to customers (often tied to buying Chinese equipment and services)[20]. Nortel, once the global leader in telecoms, is the most egregious case of a foreign company being destroyed by ruthless Chinese competition and espionage.[21]

The impetus comes from the CCP's assessment of what is needed in order for China to achieve national rejuvenation, both offensively and defensively. Responding to calls from within the US and Europe for states to "reindustrialise" as a means of breaking perceived dependency on China, the "Made in China 2025" policy identified a range of critical technology groups. The aim has been to develop and maintain a controlling market share by a 2025 deadline. This industrial policy has been further reinforced by the "Dual Circulation" strategy, whose essence can be characterised as relying upon domestic Chinese efforts and market first, and on foreign suppliers only if necessary. The corollary of these policies is that the technologies developed domestically will be aggressively pushed abroad.

A further – and most important factor – is the Military-Civil Fusion (MCF) strategy. As the name suggests, MCF seeks to drive technological innovation which would both provide market advantage and help the modernisation of the People's Liberation Army (PLA). It draws together the innovation engines of universities, military affiliated organisations, and tech companies. It also benefits from the collection of science and technology developments abroad by China's students and academics, as well as by the intelligence services. MCF represents an important factor in fulfilling Five Year Plans, Made in China 2025, and attaining the Ministry of Industry and Information Technology's goal of gaining the "strategic high ground" (see below).

---

[19] For a full discussion of the measures which the CCP uses to give Chinese companies unfair advantages see:
"2021 Report to Congress On China's WTO Compliance"
https://ustr.gov/sites/default/files/enforcement/WTO/2021%20USTR%20Report%20to%20Congress%20on%20China's%20WTO%20Compliance.pdf
and False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices
https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its/

[20] For a full discussion of the measures which the CCP uses to give Chinese companies unfair advantages see:
"2021 Report to Congress On China's WTO Compliance"
https://ustr.gov/sites/default/files/enforcement/WTO/2021%20USTR%20Report%20to%20Congress%20on%20China's%20WTO%20Compliance.pdf
and False Promises II: The Continuing Gap Between China's WTO Commitments and Its Practices
https://itif.org/publications/2021/07/26/false-promises-ii-continuing-gap-between-chinas-wto-commitments-and-its/

[21] See "China's Quest for Foreign Technology: Beyond Espionage", edited by William Hannas and Didi Kirsten Tatlow.

A TALE OF TWO COMPANIES

The Chinese government is actively driving the adoption of NB-IoT standards, and companies involved in the NB-IoT market are implementing them.[22] The relationships between Chinese technology companies that are the suppliers of IoT devices and the companies that are the suppliers of the cellular modules that enable them is key. Often conversation on risk associated with Chinese companies exporting technology globally focuses on the visible companies, overlooking the many others that sit within their supply chains.

China's two dominant players in the IoT module market are Quectel Wireless Solutions Co. Ltd. (Quectel) and Fibocom Wireless (Fibocom). Of the two, Quectel is significantly larger and is regarded as a market leader. Both companies develop products which have specific security applications. One of Quectel's cellular IoT modules, the AG215S, for example, is described on the company's website as "supports the global, US, EU and China National Security Algorithm, which can greatly boost security in vehicle communications."[23] Fibocom, meanwhile, provides 5G cellular modules for police UAVs in China.[24]

Quectel, Fibocom and China Mobile are the key suppliers of cellular IoT to a Chinese ecosystem of technology companies which includes HikVision, HiSilicon, DJI, and ZTE (these four companies are already subject to export controls in the United States). Quectel and Fibocom are intimately connected with these companies, sharing R&D, funding, staffing and ownership (one board member at HikVision is listed as a major shareholder at Quectel).This ecosystem of technology companies contributes to the CCP's Military Civil Fusion policy, playing an important role in the modernisation of the Chinese military and security apparatus.

[22] The MIIT actively drives R&D in NB-IoT standards and technologies, as summarised here: https://www.counterpointresearch.com/why-china-is-leading-nb-iot-development-globally/

[23] https://www.quectel.com/news-and-pr/quectel-unveils-new-automotive-modules-to-support-the-auto-industry-in-the-5g-era and in Chinese https://www.prnasia.com/story/269709-1.shtml

[24] https://tech.sina.cn/5g/2020-05-19/detail-iirczymk2437691.d.html and http://enet.com.cn/article/2020/0828/A202008281196473.html

Figure 4. Company Info[25]

Quectel (上海移远通信技术股份有限公司) Founded in 2010 under the leadership of its current CEO and Chairman of the Board Qian Penghe. It develops modules on almost every chip platform available in the market. This makes it particularly popular for high end integrators, as it allows product designers and private consumers to choose the right module for their device. Two-thirds of revenue comes from China, but the company is growing in North American, European and Middle Eastern markets. Quectel has maintained revenue growth of over 50 percent in each of last four years, and the company has invested in s own production lines.

Fibocom Wireless (广和通) Founded in 1999, its co-founder and current CEO is Ying Lingpeng. Fibocom focuses more on bespoke collaborations with other market leaders. For example, through this strategy it has established itself as exclusive module partner of Intel for the mobile computing market, most recently on the Intel 5G Solution 5000 wireless chipset. Fibocom has cooperated with many well-known smart security IoT companies, such as Tuya Smart, Hikvision, Qingxin Internet, to offer IoT modules for security products.

Quectel and Fibocom, like all other Chinese companies, are bound by China's national security laws. Recent state security laws, such as the 2017 Intelligence Law, have not changed the long-standing de facto practice of state power in the PRC, but have further codified the expectation that in the PRC everyone is responsible for state security.[26] PRC- based technology companies tend to acknowledge their own exposure to legal risks emanating from the current data security system being developed in the PRC in their privacy policies.[27] A Quectel privacy policy, for example, states the company does not share, transfer and publicly disclose personal data *unless* relevant laws oblige them to do so. It specifically lists as examples laws state security and national defence, public safety, public health and major public interest, criminal investigation. [28] Fibocom's searchable privacy policy, which applies to website, says "all persons entering and using the Fibocom Platform shall comply with the terms herein and the laws of the People's Republic of China. For any violation of these rules, Fibocom shall have the right to pursue legal and fair remedies."[29]

[25]Fibocom: https://min.news/en/tech/9c6ce3237797e1028926d22222a8f70c.html

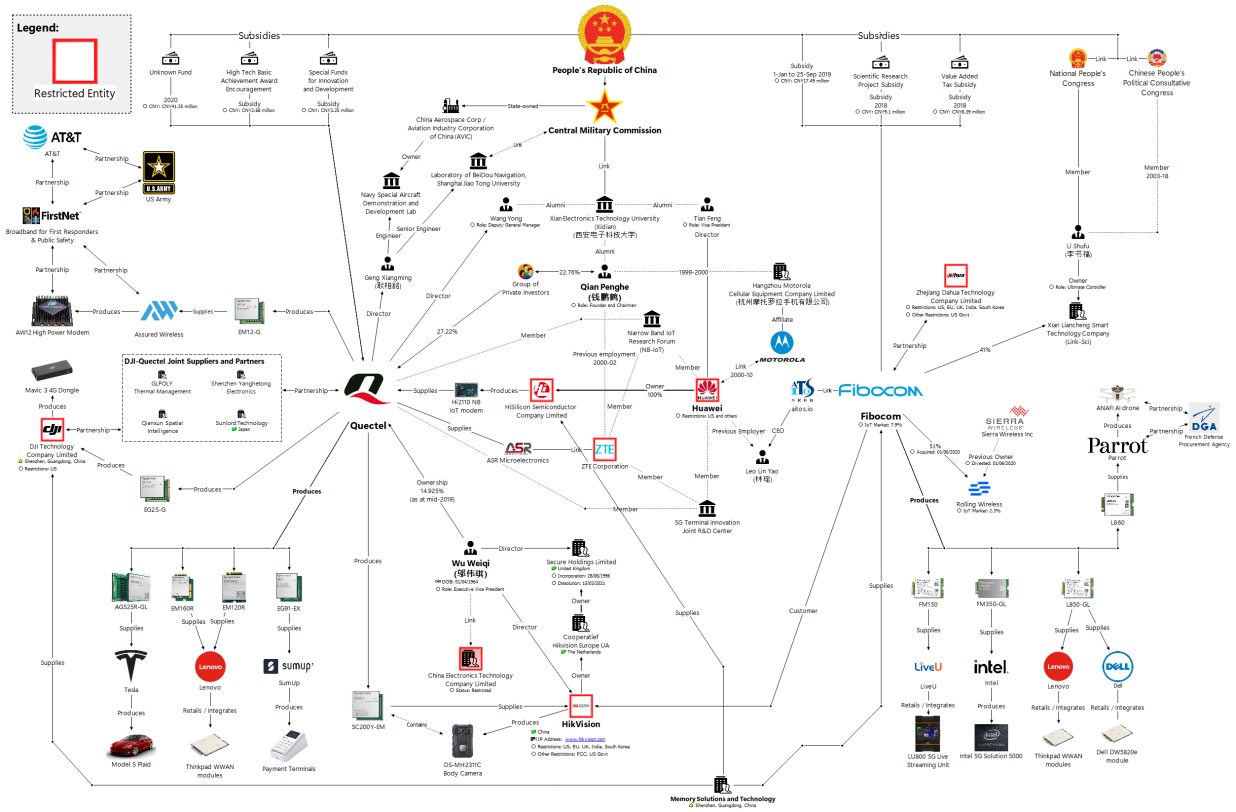
[26] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Privacy-Policies_Mapping-Chinas-Tech-Giants_Thematic-Snapshot.pdf

[27] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Privacy-Policies_Mapping-Chinas-Tech-Giants_Thematic-Snapshot.pdf

[28] https://forumschinese.quectel.com/privacy

[29] https://www.fibocom.com/en/legalnotice/index.html

Figure 5 China's IoT Ecosystem



Beyond these general risks of exposure to the Chinese party-state's demands, which apply to all PRC companies, both Quectel and Fibocom have links to other PRC companies that are suppliers for PRC IoT devices.

Figure 6. Quectel and Fibocom in Supply Chains of Restricted PRC Technology Companies

Restricted Entity	Restricted Entity Overview	Links to Quectel	Links to Fibocom
HikVision	Global market leader in Internet Protocol (IP) cameras used for surveillance and security. HikVision is facing allegations that its cameras are used in detention centres in Xinjiang. It may come under US sanctions for complicity in human rights abuses[30]. The US Treasury Department is considering placing Hikvision on its Specially Designated Nationals (SDN) list.	Quectel also had a major shareholder who was also at HikVision H, Wu Weiqi (邬伟琪)[31]	HikVision is listed as a target customer for Fibocom IoT modules, with specific reference to the production of CCTV products.[32]HikVision's cameras are now coming under increasing scrutiny by the UK government and others over concerns regarding privacy and the companies role in the repression of Uighurs in Xinjiang.
HiSilicon	A is a subsidiary of Huawei which designs silicon chips. In May 2019, the US Department of Commerce's Bureau of Industry and Security (BIS) placed HiSilicon on its Commerce Entity List[33], thereby barring its access to industry-standard chip design software, made by US company Synopsys.	Quectel has a long track record of working with HiSilicon. In February 2020 the two companies were working closely in the development of 5G industrial and consumer modules, particularly the NB-IoT module, based on the HiSilicon Boudica 150 chip.[34]	There is a regular interchange of key technologists between Fibocom and Huawei. Both companies share industry alliances and suppliers. It is a closely linked ecosystem as can be seen by the repeated overlap of memberships on

[30] FT | Hikvision shares plunge after US sanctions threat, WSJ | Opinion | Sanctions against a Chinese surveillance firm would answer a real threat

[31] http://file.finance.sina.com.cn/211.154.219.97:9494/MRGG/CNSESH_STOCK/2019/2019-6/2019-06-26/5456523.PDF

[32] https://img3.gelonghui.com/pdf/09334-29731620-df91-4d5e-a973-cdec6641e9bf.pdf

[33] Federal Register: Addition of Entities to the Entity List

[34] https://www.quectel.com/customer-stories/when-iot-cares-connected-smart-pill-dispenser; https://www.techinsights.com/products/far-1707-804

		The Quectel and HiSilicon collaboration has continued, despite US sanctions against Hisilicon. In May 2021, Quectel announced a module line of the first commercially available modules to use HiSilicon's Boudica 200 modem chip[35].	special committees and alliances.[36] [37] The HiSilicon Boudica chip is based on technology originally developed by Neul, a UK IoT research company, which Huawei purchased in 2014.[38] Its innovative, long-range radio technology intellectual property allowed Huawei, other cellular infrastructure vendors, chipset manufacturers, and mobile network operators, to promote a standard called Narrowband IoT (NB-IoT). Fibocom products have since been identified in Neul products[39] NB-IoT is a key standard for Chinese IoT manufactures with Quectel, Qualcomm, and HiSilicon jointly developing modules that use it.[40][41]
DJI	Leading drone manufacturer.	Quectel supplies IoT modules for DJI's Mavic 3 4G Dongle.[42]	is listed as customer for Fibocom IoT modules[43][44],

[35] https://www.abiresearch.com/market-research/product/7779349-quectel-the-first-to-market-with-hisilicon/

[36] The Special Committee of the Internet of Vehicles of the China Central Telecommunications Association: http://www.dvbcn.com/p/47707.html

[37] The Sanshan Science and Technology Innovation Centre: http://www.elecfans.com/iot/1394428.html

[38] https://www.theregister.com/2014/09/22/huawei_buys_cambridge_internet_of_things_pioneer_neul/

[39] https://www.techinsights.com/products/far-1707-804

[40] http://www.cww.net.cn/article?id=470251

[41] http://webcache.googleusercontent.com/search?q=cache:rpwx8N5yRe8J:www.wxioti.com/news/company/2019-12-13/761.html+&cd=36&hl=zh-CN&ct=clnk

[42] https://bbs.dji.com/thread-297234-1-1.html

[43] https://gsma.force.com/mwcoem/servlet/servlet.FileDownload?file=00P6900002oQ5tzEAC

[44] The Blockchain Module Alliance: https://www.sohu.com/a/362997679_682625

	DJI is subject to US investment and export restrictions, including the Entity List of the US Department of Commerce's BIS. In other words, DJI is seen as engaging in activities contrary to US national security.	Quectel is an industry alliance partner with DJI. The drone manufacturer is currently under significant restrictions in the US due to national security and human rights concerns.	demonstrating how China's leading cellular IoT module designers and manufacturers cooperate in the development and deployment of strategically relevant products to the global and domestic markets.
ZTE	One of China's two main exporters of telecoms equipment and services. In 2017 the US government placed ZTE on restrictive lists for violating sanctions. The company admitted the charges and paid a US$ 900 million fine.[45] A year later ZTE was found to be in violation of these conditions, and the Department of Commerce banned US companies from providing parts to ZTE for seven years. In a new settlement, ZTE paid a further US$ 1 billion fine, replaced its entire senior management in the US, and established a compliance department selected by the US Department of Justice.[46]	The founder of ZTE, Qian Penghe, is also one of the main private shareholders in Quectel. There is a regular interchange of employees. They are members of many of the same alliances including the 5G Terminal Innovation Joint R&D Centre[48]. Quectel supplies components to ASR Microelectronics which in turn is a key supplier to ZTE.	

[45] https://www.theregister.com/2017/03/07/zte_900m_fine_for_iran_dealings/

[46] https://www.engadget.com/2018-06-07-zte-export-ban-billion-dollar-fine.html

[48] http://webcache.googleusercontent.com/search?q=cache:U5xxntYRyzQJ:www.chinaunicom.com.cn/news/201904/1556087354374160355.html+&cd=32&hl=zh-CN&ct=clnk

	The company is still barred from US government contracts. US telecommunications providers may not use government funds to purchase ZTE equipment.[47]		

Fibocom and Quectel products can remain sitting within the supply chains of the national defence ecosystem of the US and allied countries. Ironically, by highlighting two specific companies, Fibocom and Quectel, we can see that company-specific approaches to assessing risk is not, as it stands, adequate enough to address IoT supply chain security issues. Huawei's relationship with Fibocom suggests a strategy which is to establish dominance in the NB-IoT market. In May 2022, Canada announced plans to ban the use of Huawei and ZTE equipment from use in 5G infrastructure, citing national security concerns Companies using equipment or managed services from the two Chinese companies have until 28 June 2024 to remove the equipment. The announcement said that the two companies 'could be compelled to comply with extrajudicial directions from foreign governments in ways that would conflict with Canadian laws or would be detrimental to Canadian interests.'[49]

While Canadian policy addresses the de facto relationship with Fibocom, it does not change Fibocom's significant presence in Canada. Fibocom has expanded into the vehicle IoT market by acquiring the Canadian company Sierra Wireless Automotive group in 2020 for UD$165 million, under the consortium Rolling Wireless. It subsequently hired Sierra Wireless management to run Rolling Wireless and overseas business, while also hiring from other module vendors to expand in the US. Fibocom is also expanding into Western markets through its relationship with Intel. The company has displaced other competitors to win designs with western PC manufacturers, such as Lenovo, Dell and HP, which now use Fibocom modules in their off the shelf computers. In the past year, Quectel launched a new original design manufacturer brand, Ikotek, targeting the US and Latin America. It is also trying to break into the overseas automotive market by placing its network access device modules in foreign electric vehicles.

UNDERSTANDING AND MITIGATING THE THREAT

Because so little work has been done on the threat from Chinese cellular IoT modules, it is difficult to point to specific examples where data has been sent back to China to the detriment of the interests of free and open countries. But given the CCP's record in other areas (there have recently been instances where Tik Tok and Huawei have assured that information is not sent to China, only for

[47] https://techonomy.com/huawei-zte-banned-from-selling-to-u-s-government/

[49] https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html

evidence to emerge that it is[50]), this is not a risk which other countries should take. CCP support for Russia, its behaviour in the Taiwan Straits and the South China Sea, its repudiation of universal values in the infamous "document no 9" and demonstration of that disregard in Hong Kong and Xinjiang should convince our policy makers that if the CCP does not represent a hostile power now, it is likely to in future. Therefore, with cellular IoT modules, it is a question of identifying the vulnerabilities and taking measures to close them off.

Dependency of free and open countries on Chinese companies would give the CCP a significant lever for use against them. We have seen how during the Covid crisis, the Party was not averse to manipulating the supply of medical goods. Hostility does not need to be carried out only in traditional armed conflict.

The threat can be broken down into four areas. This section takes a brief look at them.

1. National security threat

The national security arguments which apply to Chinese hardware and software in the telecoms, semiconductors and other sectors and upon which governments have acted apply to the IoT. This national security threat is wide ranging. Interference in CNI, or the threat thereof as a lever on policy, is at the extreme end.

The CCP could also use cellular IoT modules to harvest data and to supplement its intelligence efforts. For example, the Chinese intelligence services might not have penetration of American weapons manufacturing, but through IoT modules embedded in the supply chains and logistics system they might be able to build up a worryingly accurate picture of how many spare parts, or weapons systems have been transported and to where.

This intelligence threat could apply to attempts to recruit individuals as spies. By combining and personal and institutional data from a wide range of sources and processing it using machine learning, it would be possible to identify key government workers and their potential vulnerabilities to intelligence approaches or disruption. Chinese state hackers notoriously broke into the US Office of Personnel Management.[51] Their aim was to access personal information to help target Americans with access to classified information. It would be unwise to give Chinese companies unfettered access to similar types of information by allowing their IoT modules into our systems.

Case study - Law Enforcement Body Cams
Axon (formerly Taser) has 70 percent of the market in the US for police body cameras (as of October 2020 in 49 cities). It also supplies the US Border Patrol, US Customs, and the Drug Enforcement Agency, as well as police forces in the UK and other countries.[1]

Quectel is in the final stages of developing a custom-built design for Axon, which is currently going through certification and is likely to be deployed in the next 2-3 months. All currently-deployed devices have Sierra Wireless (Canada) modules.

[50] https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access
[51] https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

2. Economic prosperity threat

As indicated earlier, CCP industrial policy aims to ensure that Chinese companies, which must cooperate with their political masters, dominate the new technologies and industries, since this serves to advance China's economic, and thereby geopolitical, pre-eminence. This would not only reduce liberal democracies to a dangerous dependency, but would hollow out their companies. Part of this process is what might be called "venture communism", in which Chinese companies buy out foreign firms in the same field, whether in order to grow, to reduce competition[52] or to obtain technology and intellectual property. There is a particular concentration on start-up companies, whose attraction is both their new technologies and the fact that, by virtue of size, they do not appear on the radar of measures such as the UK's National Security Investment Act.

Case study - Agriculture

Farming is a critical industry. Automation helps to increase yields while decreasing labour – similar to the logic which has seen automation become the norm in the automotive industry and within large retailers like Amazon. From automated harvesters to drones for monitoring crops and watering, cellular IoT modules suit farming equipment, not least because they allow continuous connectivity in places where WiFi is inaccessible or wired networking over huge distances is impractical.

At first sight data from IoT enabled farming equipment hardly seems threatening, even in the hands of a malicious actor. But, for example, if systems extensively used Chinese modules, knowledge of current, past, and predicted trends for crop yield, the resources used on the upkeep of the land, the financial situation of the potential vendor would enable CCP backed companies to identify farming enterprises in a precarious situation and to buy them out when they are at their most vulnerable. They could be well placed in negotiations with the US on grain contracts, on buying up American expertise in farm machinery or seed technology, or in more accurately targeting sanctions on American growers for political ends.

The data generated by automated logistics, manufacturing, and transport systems would allow the holder to develop an industrial pattern-of-life of any supplies chains covered. This could be invaluable as a means of ensuring that the holder's economic interests prosper over those of a competitor. Data from the networks and systems into which these routers would be plugged would provide insights into productivity, rate and quantity of supply, and efficiency. This equates to a form of data driven insider knowledge.

Such knowledge from inside a competitor or existing infrastructure could allow a malicious actor to tune their bids for infrastructure projects or for the buyouts of competitors. It could also allow them to manage their own supply chains and market offerings in a manner which permitted them to adapt pre-emptively to the strategies and capabilities of their competitors. This would undermine the free market and the forces of supply and demand.

[52] See the report of what appears to be a deliberate attempt to buy into the UK company Nexperia and to starve it of funding in order to kill off competition, the Times, 6 August 2022. https://www.thetimes.co.uk/article/chinese-backed-nexperia-hobbled-newport-wafer-fab-to-buy-on-the-cheap-q859ztdrb

The systematic acquisition of western science and technology and the erosion of the ability of western companies to compete, if unchecked, would undermine prosperity, geopolitical strength and the values upon which democratic countries have based their systems. Ultimately economic prosperity melds into national security.

3. Data privacy threat

IoT devices are becoming increasingly commonplace within people's homes. The range of uses and the data which they collect and process are expanding, not least so that targeted marketing can be sent to their owners. Wearable technology collects health and activity data; smart kitchen appliances or multimedia devices collect information on behaviour and personal interactions; door cameras, alarm systems and security cameras equipped with machine learning monitor personal comings and goings; smart meters monitor usage of electricity and gas, which in the midst of an energy crisis brought about by state manipulation of natural resources prices for political aims is of contemporary concern.

While it may not unduly worry the average citizen if the security organs of the CCP were to be in possession of personal information, it might concern those in free and open societies who, for example, are of Uyghur extraction, have relatives in Hong Kong or might work in sensitive government positions. By collating such information and the metadata created as people interact with IoT devices, particularly of electronic payments and travel, it is possible to work out who has been meeting whom and where. This pattern-of-life information can provide deep and rich insights into our daily habits, contacts and finances. Coupled with machine learning, such data makes it possible to make

Case study – vehicle data

IoT cellular modules in vehicles are a particular worry. For example, Quectel supplies its AG525R-GL module to Tesla for the powerful 'car computers' in its Model S Plaid and Model X Plaid to manage the internal data processing. These modems have been designed for auto-related applications, such as fleet management, vehicle tracking, in-vehicle navigation system, vehicle remote monitoring, vehicle remote control, security monitoring and alarming, remote vehicle diagnostics, vehicle wireless routing and in-car entertainment.

The dangers of allowing vehicle data to come into the possession of hostile powers are clear. For example, it could be used to identify sensitive government employees by locating their place of work, their home and their meetings. In January 2023, the *i* newspaper in the UK reported that a surreptitious Chinese cellular IoT module had been discovered in UK government cars, including those used by senior government minsters. The newspaper reported, 'A hidden Chinese tracking device was found in a UK Government car after intelligence officials stripped back vehicles in response to growing concerns over spyware, **i** has been told. At least one SIM card capable of transmitting location data was discovered in a sweep of Government and diplomatic vehicles which uncovered "disturbing things", a serving security source confirmed. The geolocating device had been placed into a vehicle inside a sealed part imported from a supplier in China and installed by the vehicle manufacturer, according to the source.' [1]

predictive assessments of where a person might be or how they might act at a certain time or in a certain situation. Such a capability is a threat not just to individual liberty and freedom of choice, but to security through the increased risk of effective blackmail campaigns tailored to the very specific lifestyle of an individual target.

4. The Values Threat

Quectel's and Fibocom's work with HikVision cameras, HiSilicon semiconductors, and Huawei 5G infrastructure is important for the functioning of "smart cities". Often the term "smart cities" is a euphemism for the surveillance deployed by the CCP in Xinjiang, and increasingly in other parts of China, as well as abroad through export. They are attractive not least in Hong Kong, Africa and parts of Europe, because of the low initial cost, long term maintenance contracts, and potential savings and efficiency for local governments as a result of better information. Yet they are the central pillar of digital authoritarianism directed at minority groups within China. Their R&D and their supplier's increasingly dominant position in the market is built on the back of the work given to them by the CCP in policing the minority population in Xinjiang. This is unwholesome.

Quectel's and Fibocom's modules transfer the data captured by the more easily noticed apparatus of surveillance back to centres for processing. Using machine learning security forces attempt to identify indicators of behaviour which are seen as a threat to the CCP.

As these companies make their way into our airports, ports, cities, and road systems under the seemingly innocuous Trojan horse of "Smart Cities", they bring with them the same values which they present within mainland China. Cheap and useful though they may be, but by normalising their use within our societies we are normalising their darker side.

The same cameras, telecoms infrastructure, and 'smart' systems are increasingly being promoted to cities in free and open countries. In the UK, Milton Keynes and Bournemouth are examples.[53] The relatively low cost of networked services and capabilities which could improve traffic, logistics, or security is attractive to cities with tight budgets. But governments need to decide – quickly – whether they are happy to import CCP values.

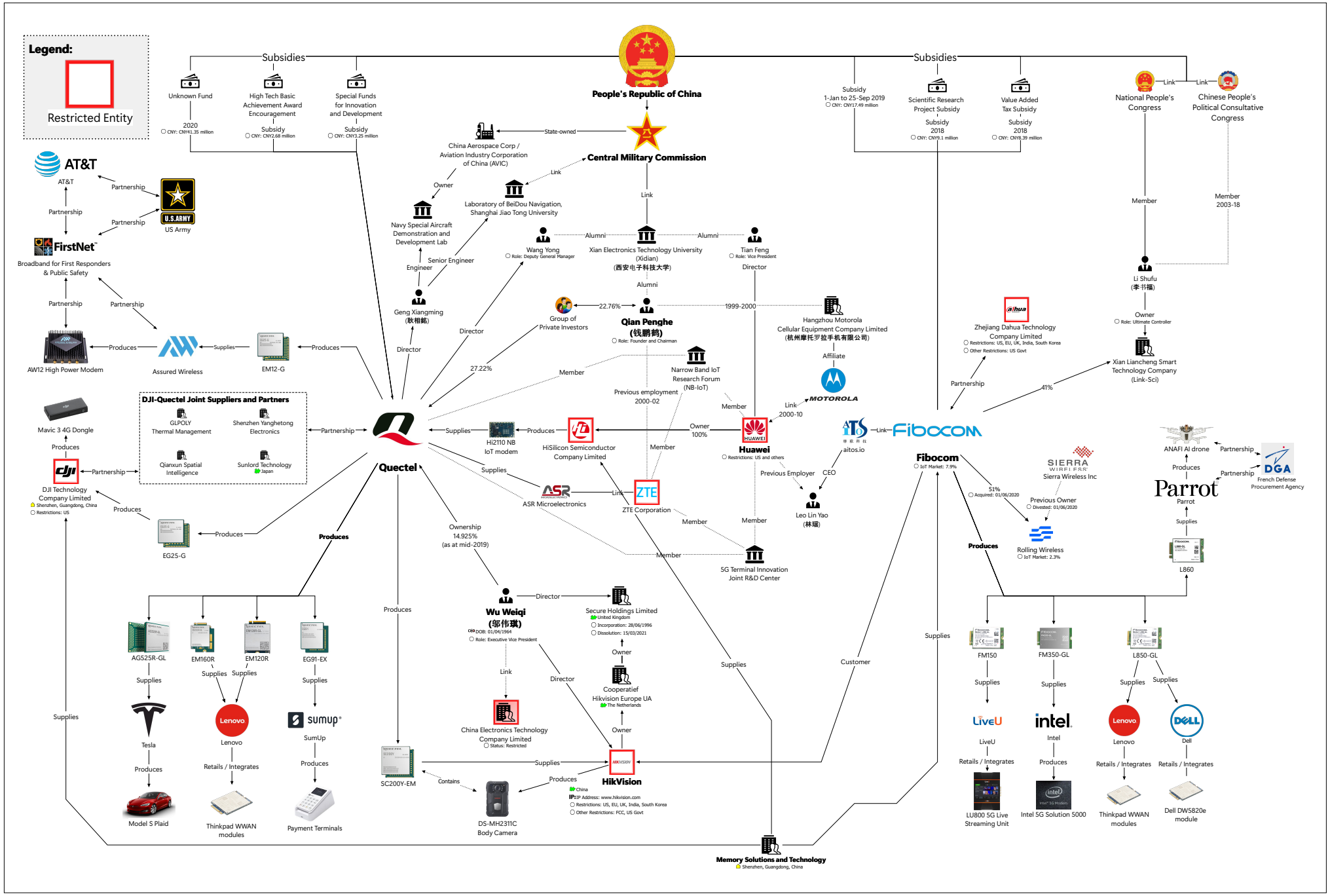
CONCLUSION

Countering these threats and mitigating the risks will also empower the domestic IoT industry in the US, UK and their allies, delivering a supply chain which enables growth and innovation. The fostering of a strong, globally competitive market for IoT companies will serve to drive industry and innovation in a manner which avoids the risks inherent in a supply chain dominated by CCP controlled companies. Fortunately, there remain a good number of American, European, and Asian players still in the market, as was not the case with Huawei, where the only other options were Erikson and Nokia.

Free nations have taken action in the areas of 5G and semiconductors. They need – urgently – to do the same in the field of IoT, to preserve the future of IoT manufacturers based in our countries, and

[53] As reported in the Financial Times two smart city deals with local authorities in the UK were cancelled at the very last minute after intervention by the NCSC and GCHQ: https://www.ft.com/content/46d35d62-0307-41d8-96a8-de9b52bf0ec3 .

to uphold national security, economic prosperity, privacy and values. The longer the delay in limiting Chinese cellular IoT modules, the more difficult and expensive it becomes to replace them. The window of opportunity is closing, but it is still open.


Legend:
Restricted Entity
People's Republic of China
Subsidies
Unknown Fund
2020
CNY: CNY41.35 million
High Tech Basic Achievement Award Encouragement
Subsidy
CNY: CNY2.68 million
Special Funds for Innovation and Development
Subsidy
CNY: CNY3.25 million
Subsidies
Subsidy
1-Jan to 25-Sep 2019
CNY: CNY17.49 million
Scientific Research Project Subsidy
Subsidy
2018
CNY: CNY9.1 million
Value Added Tax Subsidy
Subsidy
2018
CNY: CNY8.39 million
National People's Congress
Link
Chinese People's Political Consultative Congress
Member
Member
2003-18
China Aerospace Corp / Aviation Industry Corporation of China (AVIC)
State-owned
Central Military Commission
Link
Owner
Laboratory of BeiDou Navigation, Shanghai Jiao Tong University
Navy Special Aircraft Demonstration and Development Lab
Senior Engineer
Engineer
Geng Xiangming
(耿相銘)
Director
Wang Yong
Role: Deputy General Manager
Alumni
Xian Electronics Technology University (Xidian)
(西安电子科技大学)
Alumni
Tian Feng
Role: Vice President
Director
Alumni
Li Shufu
(李书福)
Owner
Role: Ultimate Controller
Xian Liancheng Smart Technology Company (Link-Sci)
41%
Partnership
Zhejiang Dahua Technology Company Limited
Restrictions: US, EU, UK, India, South Korea
Other Restrictions: US Govt
Group of Private Investors
22.76%
Qian Penghe
(钱鹏鹤)
Role: Founder and Chairman
1999-2000
Hangzhou Motorola Cellular Equipment Company Limited
(杭州摩托罗拉手机有限公司)
Affiliate
MOTOROLA
Director
27.22%
Member
Narrow Band IoT Research Forum (NB-IoT)
Previous employment
2000-02
Member
Link
2000-10
AT&T
Partnership
U.S.ARMY
US Army
FirstNet
Broadband for First Responders & Public Safety
Partnership
Partnership
Partnership
Partnership
AW12 High Power Modem
Produces
Assured Wireless
Supplies
EM12-G
Produces
Mavic 3 4G Dongle
Produces
DJI Technology Company Limited
Shenzhen, Guangdong, China
Restrictions: US
Partnership
Produces
DJI-Quectel Joint Suppliers and Partners
GLPOLY
Thermal Management
Shenzhen Yanghetong Electronics
Qianxun Spatial Intelligence
Sunlord Technology
Japan
Partnership
EG25-G
Produces
Quectel
Produces
Supplies
Hi2110 NB IoT modem
Produces
HiSilicon Semiconductor Company Limited
Owner
100%
Huawei
Restrictions: US and others
Supplies
ASR Microelectronics
Link
ZTE
ZTE Corporation
Member
Member
Member
5G Terminal Innovation Joint R&D Center
Previous Employer
CEO
Leo Lin Yao
(林瑶)
aitos.io
Link
Fibocom
Fibocom
IoT Market: 7.9%
51%
Acquired: 01/06/2020
SIERRA WIRELESS
Sierra Wireless Inc
Previous Owner
Divested: 01/06/2020
Rolling Wireless
IoT Market: 2.3%
Produces
ANAFI AI drone
Partnership
DGA
French Defense Procurement Agency
Partnership
Produces
Parrot
Parrot
Supplies
L860
AG525R-GL
EM160R
EM120R
EG91-EX
Supplies
Supplies
Supplies
Supplies
Supplies
Tesla
Produces
Model S Plaid
Lenovo
Lenovo
Retails / Integrates
Thinkpad WWAN modules
SumUp
SumUp
Produces
Payment Terminals
Produces
Ownership 14.925% (as at mid-2019)
Wu Weiqi
(邹伟琪)
DOB: 01/04/1964
Role: Executive Vice President
Director
Secure Holdings Limited
United Kingdom
Incorporation: 28/06/1996
Dissolution: 15/03/2021
Owner
Cooperatief Hikvision Europe UA
The Netherlands
Owner
Director
Link
China Electronics Technology Company Limited
Status: Restricted
SC200Y-EM
Contains
DS-MH2311C Body Camera
Supplies
Produces
HikVision
China
IP: IP Address: www.hikvision.com
Restrictions: US, EU, UK, India, South Korea
Other Restrictions: FCC, US Govt
Supplies
Supplies
Customer
Supplies
Memory Solutions and Technology
Shenzhen, Guangdong, China
FM150
FM350-GL
L850-GL
Supplies
Supplies
Supplies
Supplies
LiveU
LiveU
Retails / Integrates
LU800 5G Live Streaming Unit
intel
Intel
Produces
Intel 5G Solution 5000
Lenovo
Lenovo
Retails / Integrates
Thinkpad WWAN modules
DELL
Dell
Retails / Integrates
Dell DW5820e module

From	Relationship	To	Direction	Original Source	Archived Source
5G Terminal Innovation Joint R&D Center	Partnership With	Huawei		Link	Archived Link
5G Terminal Innovation Joint R&D Center	Partnership With	ZTE Corporation		Link	Archived Link
AG525R-GL	Is Supplier To	Tesla	A ---> B	Link	Archived Link
aitos.io	Is Director Of	Leo Lin Yao (林瑶)	A ---> B	Link	Archived Link
ASR Microelectronics	Link	ZTE Corporation		Link	[No archive]
Assured Wireless	Is Supplier Of	AW12 High Power Modem	A ---> B	Link	[No archive]
Assured Wireless	Partnership With	Broadband for First Responders & Public Safety	A <---> B	Link	Archived Link
AT&T	Partnership With	US Army	A <---> B	Link	Archived Link
AW12 High Power Modem	Partnership With	Broadband for First Responders & Public Safety	A <---> B	Link	Archived Link
Broadband for First Responders & Public Safety	Partnership With	AT&T	A <---> B	Link	Archived Link
Broadband for First Responders & Public Safety	Partnership With	US Army	A <---> B	Link	Archived Link
Central Military Commission	Link	Laboratory of BeiDou Navigation, Shanghai Jiao Tong U	A <---> B	Link	[No archive]
Central Military Commission	Owns	China Aerospace Corp / Aviation Industry Corporation	A ---> B	Link	[No archive]
China Aerospace Corp / Aviation Industry Corporation	Owns	Navy Special Aircraft Demonstration and Developmen	A ---> B	Link	Archived Link
Cooperatief Hikvision Europe UA	Owns	Secure Holdings Limited	A ---> B	Link	[No archive]
Dell	Is Supplier To	Dell DW5820e module		Link	Archived Link
DJI Technology Company Limited	Is Supplier Of	Mavic 3 4G Dongle	A ---> B	Link	Archived Link
DJI Technology Company Limited	Partnership With	GLPOLY Thermal Management	A <---> B	Link	Archived Link
EG25-G	Is Supplier Of	DJI Technology Company Limited	A ---> B	Link	Archived Link
EG91-EX	Is Supplier To	SumUp	A ---> B	Link	Archived Link
EM120R	Is Supplier To	Lenovo	A ---> B	Link	[No archive]
EM12-G	Is Supplier To	Assured Wireless	A ---> B	Link	[No archive]
EM160R	Is Supplier To	Lenovo	A ---> B	Link	[No archive]
Fibocom	Is Supplier To	L860	A ---> B	Link	[No archive]
Fibocom	Link	aitos.io		Link	[No archive]
Fibocom	Owns	Xian Liancheng Smart Technology Company (Link-Sci	A ---> B	Link	Archived Link
Fibocom	Owns	Rolling Wireless	A ---> B	Link	Archived Link
Fibocom	Partnership With	HikVision	A ---> B	Link	Archived Link
Fibocom	Partnership With	Zhejiang Dahua Technology Company Limited	A <---> B	Link	[No archive]
FM150	Is Supplier To	LiveU	A ---> B	Link	Archived Link
FM350-GL	Is Supplier To	Intel	A ---> B	Link	[No archive]
French Defense Procurement Agency	Partnership With	ANAFI AI drone	A <---> B	Link	Archived Link
Geng Xiangming	Link	Navy Special Aircraft Demonstration and Developmen	A ---> B	Link	Archived Link
Geng Xiangming	Link	Laboratory of BeiDou Navigation, Shanghai Jiao Tong U	A ---> B	Link	Archived Link
Group of Private Investors	Link	Quectel	A ---> B	Link	Archived Link
Hangzhou Motorola Cellular Equipment Company Limi	Link	Motorola Group		Link	Archived Link
Hi2110 NB IoT modem	Is Supplier To	Quectel	A ---> B	Link	Archived Link
High Tech Basic Achievement Award Encouragement	Financial Transaction To	Quectel		Link	Archived Link
HikVision	Is Supplier Of	DS-MH2311C Body Camera	A ---> B	Link	[No archive]
HikVision	Owns	Cooperatief Hikvision Europe UA	A ---> B	Link	[No archive]
Huawei	Is Subscriber Of	Narrow Band IoT Research (NB-IoT)		Link	Archived Link
Huawei	Link	Motorola Group	A <---> B	Link	Archived Link
Huawei	Link	Leo Lin Yao (林瑶)	A ---> B	Link	Archived Link
Huawei	Owns	HiSilicon Semiconductor Company Limited	A ---> B	Link	Archived Link
Intel	Is Supplier Of	Intel 5G Solution 5000	A ---> B	Link	[No archive]
L850-GL	Is Supplier To	Lenovo	A ---> B	Link	[No archive]
L850-GL	Is Supplier To	Dell	A ---> B	Link	Archived Link
L860	Is Supplier To	Lenovo	A ---> B	Link	[No archive]
Lenovo	Is Supplier To	Thinkpad WWAN modules	A ---> B	Link	[No archive]
Lenovo	Is Supplier To	Thinkpad WWAN modules	A ---> B	Link	[No archive]
Li Shufu (李书福)	Is Subscriber Of	National People's Congress		Link	Archived Link
Li Shufu (李书福)	Is Subscriber Of	Chinese People's Political Consultative Congress		Link	Archived Link
Li Shufu (李书福)	Owns	Xian Liancheng Smart Technology Company (Link-Sci	A ---> B	Link	Archived Link
LiveU	Is Supplier To	LU800 5G Live Streaming Unit	A ---> B	Link	Archived Link
Memory Solutions and Technology	Is Supplier To	HiSilicon Semiconductor Company Limited	A ---> B	Link	Archived Link
Memory Solutions and Technology	Is Supplier To	DJI Technology Company Limited	A ---> B	Link	Archived Link
Memory Solutions and Technology	Is Supplier To	Fibocom	A ---> B	Link	Archived Link
Parrot	Is Supplier Of	ANAFI AI drone	A ---> B	Link	[No archive]
Parrot	Partnership With	French Defense Procurement Agency	A <---> B	Link	Archived Link
People's Republic of China	Financial Transaction To	High Tech Basic Achievement Award Encouragement		Link	Archived Link
People's Republic of China	Financial Transaction To	Special Funds for Innovation and Development		Link	Archived Link
People's Republic of China	Financial Transaction To	Fibocom		Link	[No archive]
People's Republic of China	Link	Chinese People's Political Consultative Congress		Link	Archived Link
People's Republic of China	Link	Central Military Commission	A ---> B	Link	Archived Link
People's Republic of China	Link	National People's Congress		Link	Archived Link
Qian Penghe (钱鹏鹤)	Link	Hangzhou Motorola Cellular Equipment Company Limited (杭州摩扌		Link	Archived Link
Qian Penghe (钱鹏鹤)	Link	Group of Private Investors	A <---> B	Link	Archived Link
Qian Penghe (钱鹏鹤)	Link	Xian Electronics Technology University (Xidian) (西安电子科技大学		Link	Archived Link
Qian Penghe (钱鹏鹤)	Link	ZTE Corporation		Link	Archived Link
Quectel	Is Director Of	Wang Yong	A ---> B	Link	Archived Link
Quectel	Is Director Of	Geng Xiangmin	A ---> B	Link	Archived Link
Quectel	Is Subscriber Of	Narrow Band IoT Research (NB-IoT)		Link	Archived Link
Quectel	Is Supplier To	ASR Microelectronics		Link	Archived Link
Quectel	Partnership With	5G Terminal Innovation Joint R&D Center		Link	[No archive]
Quectel	Partnership With	GLPOLY Thermal Management	A <---> B	Link	Archived Link
SC200Y-EM	Is Supplier To	HikVision	A ---> B	Link	[No archive]
SC200Y-EM	Link	DS-MH2311C Body Camera	A <---> B	Link	[No archive]
Scientific Research Project Subsidy	Financial Transaction To	Fibocom		Link	Archived Link
Sierra Wireless Inc	Owns	Rolling Wireless	A ---> B	Link	Archived Link
Special Funds for Innovation and Development	Financial Transaction To	Quectel		Link	Archived Link
SumUp	Is Supplier Of	Payment Terminals	A ---> B	Link	Archived Link
Tesla	Is Supplier Of	Model S Plaid	A ---> B	Link	Archived Link
Tian Feng	Is Director Of	Huawei		Link	Archived Link
Unknown Fund	Financial Transaction To	Quectel	A ---> B	Link	Archived Link
Value Added Tax Subsidy	Financial Transaction To	Fibocom		Link	Archived Link
Wu Weiqi (邬伟琪)	Is Director Of	Secure Holdings Limited	A ---> B	Link	[No archive]
Wu Weiqi (邬伟琪)	Is Director Of	HikVision	A ---> B	Link	Archived Link
Wu Weiqi (邬伟琪)	Link	China Electronics Technology Company Limited	A ---> B	Link	Archived Link
Wu Weiqi (邬伟琪)	Link	Quectel	A ---> B	Link	Archived Link
Xian Electronics Technology University (Xidian) (西安电	Link	Wang Yong		Link	Archived Link
Xian Electronics Technology University (Xidian) (西安电	Link	Tian Feng		Link	Archived Link
Xian Electronics Technology University (Xidian) (西安电	Link	Central Military Commission		Link	Archived Link
ZTE Corporation	Partnership With	Narrow Band IoT Research (NB-IoT)		Link	Archived Link