



**COALITION ON
SECURE TECHNOLOGY**

REPORT

CIMs Risk in UK Agriculture

Assessing the national security and food security implications of Chinese-manufactured Cellular Internet-of-Things Modules in UK agricultural technology

Coalition on Secure Technology
September 2026

Contents

Executive Summary	3
CIMs in Agriculture	3
Key Security Threats	4
1. Remote Access and Cyber Intrusion Risks	4
2. Food Security Implications	4
3. Supply Chain Coercion and Economic Leverage.....	5
4. Data Collection and Strategic Intelligence Gathering.....	6
Challenges in the Agricultural Sector.....	6
Assessing the Severity of the Threat	7
Conclusion.....	8

Executive Summary

The increasing use of Chinese-manufactured Cellular Internet-of-Things Modules (CIMs) within UK agricultural technology presents a growing economic and national security challenge.

Agriculture is an increasingly technological business. Automated systems rely on connectivity via the internet, and that connectivity is provided by CIMs.

CIMs are embedded cellular communications modules that allow equipment, sensors and software platforms to connect to mobile networks to transmit data. They are now commonly found in precision agriculture systems, autonomous machinery, livestock monitoring equipment, environmental sensors, irrigation systems, drones and supply-chain management tools.

CIMs represent a critical security concern. They are gateways for data and instructions to flow through. Manufacturers send remote firmware updates to CIMs deployed in devices. This enables them to insert malware, collect data covertly, or disrupt and disable machines or systems. This is not fiction. When the Russians stole agricultural machinery from Ukraine after the invasion, the manufacturer John Deere remotely disabled the machines via instructions passed through the CIM.

Although agriculture is not traditionally viewed as critical national infrastructure on the same level as energy or telecommunications, the increasing digitisation of food production is making agricultural systems strategically important to the UK's food security ecosystem. As a result, vulnerabilities in connected agricultural technologies could have widespread consequences for food security across the UK.

CIMs in Agriculture

Modern farming increasingly relies on connected technologies for:

- Precision fertiliser and pesticide application
- Remote monitoring of livestock health
- Automated irrigation systems
- GPS-guided tractors and autonomous vehicles
- Grain storage monitoring
- Agricultural drones
- Farm management software integrated with sensors

These systems generate large volumes of data about farming operations, productivity and the environment. Many of these systems depend on CIM-enabled connectivity to transmit information to cloud platforms and receive software updates.

CST argues that the growing ubiquity of CIMs means they should be viewed as part of a broader category of emerging critical infrastructure because they sit inside technologies that underpin economic activity and societal resilience.

Key Security Threats

1. Remote Access and Cyber Intrusion Risks

Unlike many other types of electronic components, CIMs remain connected throughout their operational lives. Manufacturers can deploy firmware over-the-air updates to modules after installation. This means the trustworthiness of the manufacturer remains relevant throughout the device's lifecycle.

If vulnerabilities were introduced deliberately or unintentionally through software updates, attackers could potentially:

- Disrupt sensor networks
- Manipulate agricultural data
- Disable connected equipment
- Create pathways into wider farm IT systems
- Interfere with automated operations

2. Food Security Implications

Food security is increasingly recognised as an element of national resilience.

Were Chinese-made CIMs to achieve dominant market penetration across agricultural equipment, a future geopolitical crisis could create vulnerabilities including:

- Supply disruption of replacement components
- Restrictions on software/firmware support
- Reduced availability of security updates
- Dependence on foreign-controlled technology ecosystems

The CST has repeatedly warned that China seeks a dominant position in the CIM market and that overreliance on a limited number of suppliers based in a single country creates strategic vulnerabilities. Chinese manufacturers currently have around 70% of the global market for CIMs.

This pattern is not unique to CIMs. Beijing has pursued the same strategy of state-backed capital and rapid scale-up to secure dominant global market share in other strategic sectors, including solar power, electric vehicles and batteries, and is now applying it to food and agricultural technology. Chinese CIM dominance should be understood as part of this wider industrial strategy, rather than as an isolated feature of a single component market.¹

Agriculture may be particularly exposed because farmers often operate equipment for many years, making rapid replacement difficult and costly.

3. Supply Chain Coercion and Economic Leverage

CIMs manufacturing is overwhelmingly located in China. Major suppliers such as Quectel and Fibocom have expanded their position in global markets, supplying modules used across multiple sectors.

Should geopolitical tensions escalate, the Chinese government could potentially exploit this market concentration through:

- Export controls
- Supply restrictions
- Licensing limitations
- Software support withdrawal

For UK agriculture, this could affect everything from precision farming equipment to logistics and storage systems, leading to operational disruption during periods of geo-political tension.

Official Chinese state media confirm that this expansion reflects deliberate state strategy rather than incidental market growth. The 15th Five-Year Plan (2026–2030) explicitly calls for promoting high-quality development in the agricultural machinery and equipment sector, and Chinese customs data cited by state media show agricultural machinery exports surging 32.3% year-on-year to 67.4 billion yuan in 2025, with some manufacturers now drawing more than 80% of their revenue from overseas sales.

The same reporting confirms that exported equipment is increasingly IoT-enabled, and that export contracts routinely bundle hardware with ongoing software support: one Shandong drone manufacturer's agreement with a Kazakh cotton farm covers not only drone supply but also software

¹Ambrose Evans-Pritchard, "China's plan to dominate global food supply chains", The Daily Telegraph, 18 August 2026: <https://www.telegraph.co.uk/business/2026/08/18/china-aiming-for-global-dominance-of-mass-food-production/>.

support, pilot training and personnel management. This is, in the Chinese state's own words, the pattern of embedded technological and software dependency this report identifies as a strategic risk.²

This mechanism is not hypothetical for UK critical infrastructure either. The Port of Felixstowe, Britain's largest container port, has for several years installed remote-controlled ship-to-shore cranes manufactured by Shanghai Zhenhua Heavy Industries (ZPMC), a Chinese state-owned company that supplies around 80% of the equivalent cranes used at ports across the United States.

A congressional investigation in the United States found unauthorised cellular modems installed on ZPMC cranes that were not included in the original equipment specification and could bypass port firewalls, the same category of concern this report identifies for agricultural CIMs: connectivity embedded in critical infrastructure hardware that was neither disclosed to, nor requested by, the end user.³

4. Data Collection and Strategic Intelligence Gathering

A further concern is the ability of embedded modules to collect and transmit sensitive information.

Aggregated data sets from across the sector could provide a detailed picture of the UK's national food production capacity and vulnerabilities. For a hostile foreign state, access to nationwide agricultural datasets could enhance economic intelligence, improve understanding of supply-chain dependencies, and identify pressure points within the UK's food production system.

Agricultural systems can reveal:

- Crop yields and production forecasts
- Livestock populations
- Water usage patterns
- Farm supply chains
- Locations of strategic food assets
- Land usage trends

²Xinhua, "China's farm machinery manufacturers expand global reach amid exports surge", State Council Information Office (english.scio.gov.cn), 17 April 2026: http://english.scio.gov.cn/chinavoices/2026-04/17/content_118442873.html.

³Port of Felixstowe / Hutchison Ports, "Remote control gantry cranes at Port of Felixstowe": <https://www.portoffelixstowe.co.uk/2018/04/10/remote-control-gantry-cranes-at-port-of-felixstowe/>; and CBS News, "Chinese cranes at U.S. ports raise homeland security concerns", 12 February 2025: <https://www.cbsnews.com/news/chinese-cranes-at-u-s-ports-raise-homeland-security-concerns/>.

Challenges in the Agricultural Sector

Three factors in UK farming make CIM risks especially difficult to manage:

Scale: Thousands of farms may deploy connected devices from diverse suppliers.

Visibility: Farmers often purchase equipment without knowing which communications modules are embedded within it.

Longevity: Agricultural machinery tends to be retained for long periods, making replacement programmes expensive and slow.

This exposure is compounded by a policy gap. Food has long been formally designated as one of the UK's critical national infrastructure sectors, alongside energy, telecommunications and transport.⁴

Yet agricultural technology is the one part of that critical national infrastructure that has not received a security response comparable to other sectors. Huawei equipment was ordered stripped from UK 5G networks from 2020, and Hikvision and Dahua cameras were banned from central government sites in 2022 on national security grounds.⁵

Agriculture is also not among the 17 sectors currently designated as sensitive under the National Security and Investment Act 2021, unlike defence, energy, communications and transport, meaning foreign acquisitions of UK agri-tech suppliers do not attract the same mandatory Government scrutiny as equivalent acquisitions in those other critical national infrastructure sectors. Connected agricultural technology has, in effect, been treated as a lower priority than comparable critical national infrastructure despite carrying similar risks.⁶

Assessing the Severity of the Threat

The threat should not be overstated. There is currently no direct evidence that Chinese CIMs have been actively used to sabotage agricultural systems in the UK. However, the UK Government should take seriously the emergence of strategic dependencies and latent vulnerabilities in the domestic food production sector. Restrictions imposed by the Chinese Communist Party on the supply of rare

⁴National Audit Office, "Resilience of the UK food supply chain to disruptions": <https://www.nao.org.uk/work-in-progress/resilience-of-the-uk-food-supply-chain-to-disruptions/>.

⁵Council on Foreign Relations, "The United Kingdom Bans Huawei From 5G Networks", 14 July 2020: <https://www.cfr.org/articles/united-kingdom-bans-huawei-5g-networks-0>; and TechMonitor, "Hikvision ban: UK government blocks Chinese CCTV cameras": <https://www.techmonitor.ai/government-computing/hikvision-ban-uk-government-oliver-dowden/>.

⁶Norton Rose Fulbright, "The UK's new NSI regime: What do you need to know?": <https://www.nortonrosefulbright.com/en/knowledge/publications/c8b20a65/the-uks-new-nsi-regime-what-do-you-need-to-know>.

earths are a warning that, where China sees an opportunity to exploit a dependency to advance its geopolitical aims, it will not hesitate to use that leverage.

This is not a purely theoretical risk. In August 2026, it emerged that cameras on Royal Navy surveillance drones used by UK special forces had been covertly transmitting signals to an IP address in China, forcing the Ministry of Defence to strip all internet connectivity from the units. The incident, involving Chinese-made components embedded in sensitive equipment, illustrates precisely the mechanism of concern this report identifies for agricultural technology: the same class of embedded connectivity, once thought benign, quietly phoning home.⁷

Conclusion

The presence of Chinese-manufactured CIMs in UK agricultural technology creates a multifaceted security challenge that extends beyond traditional cyber security. The principal risks involve systemic dependence, supply-chain leverage, the possibility of future remote disruption through connected devices and data/intelligence gathering. As agriculture becomes more digitised and central to food security, these risks become increasingly relevant to broader questions of UK economic and national resilience.

The UK Government should treat connected agricultural technology as an emerging national resilience threat. It should develop a long-term strategy for reducing dependence on high-risk, foreign-controlled communications components across all sectors, including agriculture. Such a strategy should include a defined concept of a "trusted supplier" for CIMs.

⁷Richard Holmes, "Spy cameras on Navy drones secretly sent data to China", The Daily Telegraph, 9 August 2026: <https://www.telegraph.co.uk/news/2026/08/09/spy-cameras-on-navy-drones-secretly-sent-data-to-china/>.