Heligan
STRATEGIC
INSIGHTS

China's espionage penetration and the UK defence sector

In recent years the UK has been wrestling with a persistent, and evolving reality. That is, espionage is no longer a relic of the Cold War, but a constantly changing threat, and that this is especially true when it comes from Beijing.

As China comes to the end of its 14th Five-Year Plan, the stated ambition to transform the Chinese state and its military-industrial complex into a globally dominant force of innovation, intelligence-enabled operations, and advanced manufacturing that is self-reliant, seems to have been delivered. In plain terms, China has actively closed gaps with the West in its technological and defence capability and has been more than willing to reach beyond its borders to do so.

As attention in China turns to the next Five-Year Plan, the trajectory would appear to be more, not less, intense. The next decade will likely see an acceleration in activity in the same key domains of aerospace, autonomous systems, AI, advanced manufacturing, intelligent operations and space.

That means the UK government and the defence tech community must operate on some important 'time-unfriendly' assumptions: that our adversaries are going to race ahead still further, our visibility of key advances may be less visible than ever before, and that China's access points to new markets will expand.

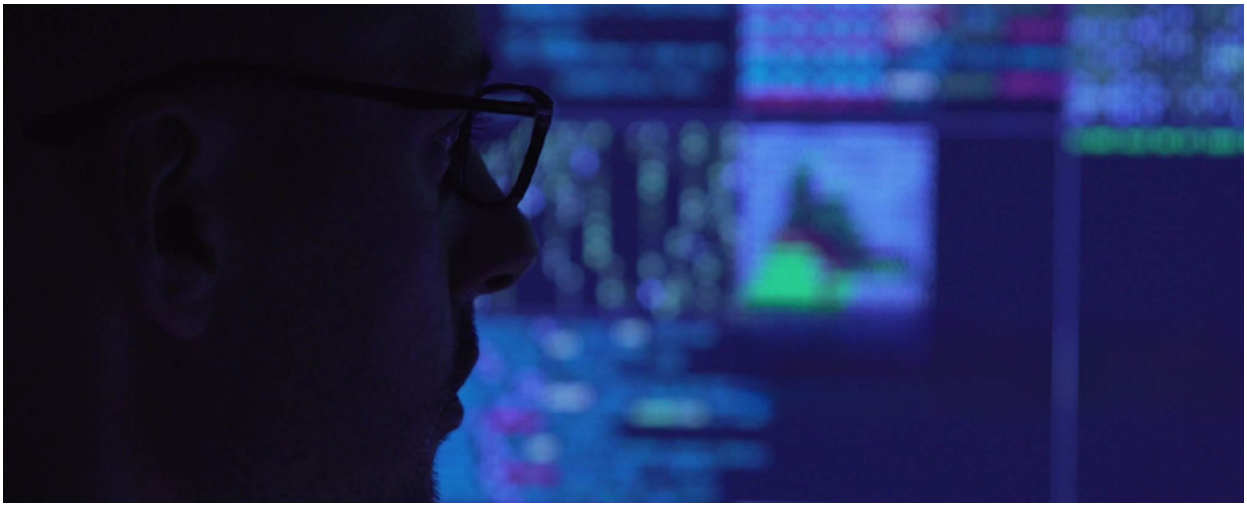
It also means that any knowledge of Chinese strategy really does matter – building an understanding of where China is trying to go gives windows into where espionage collection will be aimed. That gives defence Primes, SMEs, policy stakeholders and those charged with countering state espionage directly, the start of a strategic advantage – if we can collectively wake up to it, that is.

> Even traditionally covert activity has become more visible, with fake job adverts, recruitment gambits, and subtle supply chain infiltration now part of the standard playbook.
>
> HELIGAN INTELLIGENCE

For the UK, the implication is stark. The collection-and-influence vectors China exerts are already familiar: cyber intrusion, talent pipeline coercion, supply-chain entanglements, and academic collaboration. But these vectors are now more deeply entwined with the defence industrial base, dual-use technology flows, and things that used to sit uncomfortably between 'commercial innovation' and 'national security' than ever before.

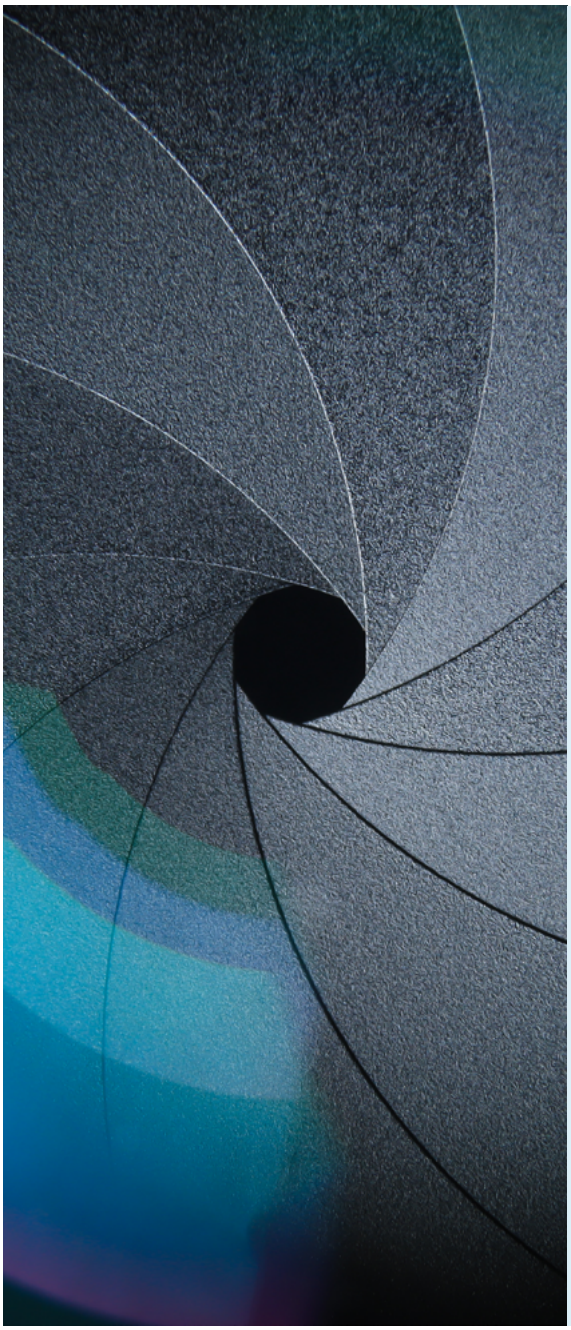
The collapse of the prosecution of two UK nationals accused of spying for China in October 2025, served as a timely reminder that while the threat is real, it is also hugely complex and interwoven with political and diplomatic maneuvering, economic engagement, and a defence-industrial reliance. We are still not getting it right!

In the same month, the MI5 Director-General underscored the point, describing Chinese state actors as posing a "daily threat" to the UK. Soon after, new guidance was issued to parliamentary, academic, and public-sector bodies warning of espionage and foreign interference by Chinese, and other state-linked entities. These approaches increasingly arrive through familiar channels such as research collaborations, social-engineering attempts, and investment overtures. Even traditionally covert activity has become more visible, with fake job adverts, recruitment gambits, and subtle supply chain infiltration now part of the standard playbook.



The UK is under no illusions about the scale of the challenge. Yet the recent intelligence dilemmas and legal setbacks make one thing unmistakably clear: the threat from Chinese espionage in the defence sector is not theoretical. It is woven into the strategic fabric of China's national plans and aligned precisely with the UK's industrial and research strengths. For UK businesses, agencies, and universities across the defence and national security ecosystem, the message is equally clear that resilience, visibility, and strategic hygiene are now mission-critical.

Security can no longer be treated as an afterthought. The question is not whether you will be targeted, but when – and how ready you'll be when it happens.



Heligan's top 5 vulnerabilities for UK defence

1. **Artificial intelligence** and data pipelines underpinning decision-support tools and autonomous systems will be primary espionage targets.
2. **Quantum-ready communications** and secure timing/sensing technologies in UK testbeds will attract intensified foreign collection.
3. **Semiconductor and sensor supply chains**, especially in small and mid-tier UK firms, will remain a high-risk access vector.
4. **Dual-use space capabilities**, including satellite design, data, and autonomy, will be increasingly contested.
5. **Investment and talent pipelines** will continue to serve as proxy access points – foreign VC and 'strategic partnerships' should be vetted through security lenses, not commercial optimism.