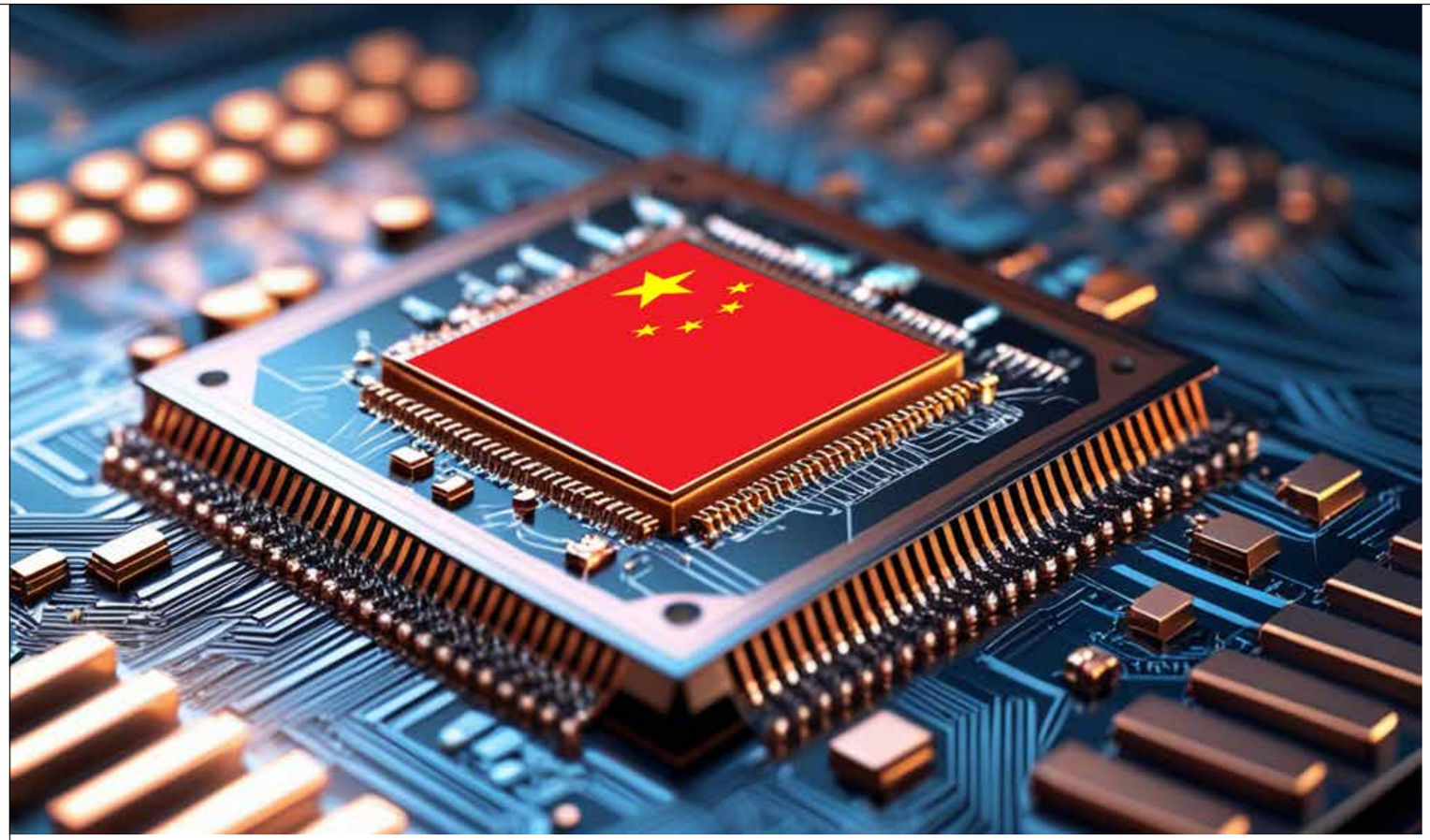

Picture credit: AdobeStock

TAKING CONTROL

Heligan Group *examines how China's tech ambitions and intelligence efforts are placing UK national security at risk*

At its core, the central goal of the People's Republic of China (PRC) is simple: to maintain the dominance of the Chinese Communist Party (CCP). Every aspect of Chinese policy, whether that be economic, technological or geopolitical, serves this singular purpose. Technological progress, foreign partnerships, military modernisation and global influence campaigns are all subordinate to the overarching objective of CCP survival and supremacy.

A major milestone on this path is China's goal of becoming the world's leading economic and technological power by 2049, marking the centenary of the PRC's founding. To achieve this, Beijing is seeking to reshape the international order in ways that conflict with the values underpinning UK national security: democratic governance, the rule of law, individual rights and market openness.

Domestically, China has consolidated digital authoritarianism, using AI-enabled surveillance, big data and social control to pre-empt dissent. Internationally, it competes for dominance across strategic sectors including AI, quantum computing, biotechnology and advanced manufacturing. The Chinese state's pursuit of "civil-military fusion" ensures that every technological advance has a potential dual-use application, integrating civilian innovation into military and intelligence capabilities.

While China maintains a publicly cordial relationship with Russia, the partnership is one of convenience rather than deep trust. Beijing benefits from Moscow's global disruption, but keeps its distance from direct entanglement. The relationship is transactional and often opaque, a chessboard of overlapping but contradictory strategic goals. At times, China positions itself as a neutral actor, even as it gains from Russian weakness and isolation.

UK industries depend on Chinese components and systems at almost every tier

Beijing's global strategy relies on a complex web of such alliances, ideologically inconsistent, but strategically useful. Through forums like the Shanghai Cooperation Organisation, the Belt and Road Initiative and the BRICS grouping, China expands influence while hedging against Western cohesion.

China sees strategic opportunity in emerging global domains. Despite having no territorial claims in the polar North, Beijing calls itself a "near-Arctic state" and is investing heavily in Arctic research, shipping routes and potential energy exploitation. In space, China's launch cadence, lunar ambitions and anti-satellite (ASAT) capabilities are increasing. In cyber space, Beijing operates the world's most extensive state-backed cyber espionage and influence operation ecosystem, targeting commercial secrets, research institutions, government infrastructure, and the global Chinese diaspora. Jeremy Fleming (the former Director of GCHQ) has been clear: "China is not just seeking progress, it is seeking control of technologies, of markets and ultimately of states."

KEEP YOUR FRIENDS CLOSE

A consistent theme in China's approach is strategic ambiguity. It will say one thing and do another, leveraging the West's preference for transparency, rules-based conduct and economic openness. The UK, like many democracies, has long underestimated the extent to which China will exploit this openness, legally or otherwise, to achieve its aims.

China has already benefited from years of close economic ties with Britain, using the openness of the UK to gain knowledge and access to markets. Through both legal and illegal means, China has moved closer to its technological and industrial goals. China's Ministry of State Security (MSS), People's Liberation Army (PLA) intelligence branches and affiliated entities like the United Front Work Department run a global network of influence and collection. From cyber intrusions to talent recruitment and IP theft, the Chinese intelligence machine is increasingly effective.

China's economic integration with global supply chains has created profound vulnerabilities. From rare earth minerals and pharmaceuticals to semiconductors and telecommunications equipment, UK industries depend on Chinese components and systems at almost every tier. This dependency creates a latent coercive lever that Beijing could exploit during times of crisis or geopolitical tension.

China's strategy of acquiring or investing in critical infrastructure and companies, including through seemingly innocuous minority stakes or partnerships, has given rise to fears over operational control, data exfiltration and national resilience. The UK's response through the National Security and Investment Act (2021) is an important tool, but remains under-resourced and lacking transparency according to Heligan's own sector experts.

Furthermore, we strongly believe that resilience means more than identifying exposure. It requires strategic initiatives such as active reshoring, diversification of suppliers and greater investment in sovereign capabilities, particularly in sectors such as AI, energy storage, defence tech and microelectronics.

China's increasingly assertive posture in global technology and security affairs, while deeply concerning, has also clarified and energised the strategic response of the UK and its allies. In pushing so aggressively to dominate key technologies, Beijing has inadvertently catalysed a wave of renewed cooperation between Western democracies, particularly among members of the Five Eyes alliance, NATO and G7. This has enabled a more focused approach to export controls, cyber cooperation and technology safeguarding.

In the UK, this shift has brought into sharper view the importance of technological sovereignty and strategic resilience. Where once globalisation led to cost-driven supply chain outsourcing, recent years have seen a decisive tilt toward reshoring critical industries, such as semiconductor fabrication, AI infrastructure and rare earth processing. Governments are also investing more in start-up and scale-up ecosystems, especially those focused on dual-use technologies in areas like quantum, cyber and space. These developments present an innovation dividend that may not have been realised without the geopolitical urgency of China's rise.

THIS WILL BE A LONG CAMPAIGN REQUIRING SUSTAINED EFFORT, INVESTMENT AND RESOLVE

This realignment has, however, produced clear losers as well. Academic institutions, long dependent on international collaboration, including with China, are increasingly constrained by national security considerations and restrictions on sensitive research partnerships. Large multinational corporations, particularly those deeply invested in or dependent on the Chinese market, face mounting compliance burdens, reputational risks and supply instability. And in the Global South, several countries that have welcomed Chinese investment through programmes like the Belt and Road Initiative are finding themselves locked into debt arrangements or reliant on Chinese technology ecosystems, potentially undermining their long-term autonomy.

Yet amid this contest, there is a growing consensus that values-aligned innovation, rooted in transparency, security and democratic norms, can be a source of competitive advantage. Those nations that can adapt quickly, foster resilient industries and manage risk intelligently will be best placed to thrive in this emerging multipolar tech order.

The Intelligence and Security Committee (ISC) 2023 report on China marked a critical shift. For years, warnings from MI5, MI6 and GCHQ had gone unheeded amid political and commercial priorities. The ISC's findings brought long-suppressed concerns to the forefront and were welcomed by all three agency heads.

For two decades, UK national security focused primarily on counter-terrorism, Russia and digital transformation. Now, China is the principal long-term strategic threat. While terrorism, organised crime and state-based cyber attacks remain concerns, countering Chinese influence, across government, academia, infrastructure and business has become a priority.

The UK will deepen cooperation with Five Eyes allies, especially the US, Australia and Canada, who have already taken tougher stances on Chinese malign activity. But senior intelligence leaders are clear: this will be a long campaign requiring sustained effort, investment and resolve.

For UK industry and innovators, this shift creates both risk and opportunity. Areas like AI assurance, secure communications, threat detection and resilient supply chains will grow in strategic relevance. The UK's startup and scale-up community, if properly supported, can help defend the country's technological edge.

THE NATIONAL SECURITY AND INVESTMENT ACT IS UNDER RESOURCED AND LACKS TRANSPARENCY

FUTURE OUTLOOK: UK–CHINA RELATIONS

Looking ahead, the relationship between the UK and China is likely to remain characterised by strategic caution, managed engagement and increasing competition. While both nations continue to share strong economic ties and interdependent trade relationships, trust in the broader political and security context has definitely eroded. It is Heligan's view that future engagement will be selective and conditional, shaped by national security interests, technological sovereignty and alliance commitments.

KEEPING BOUNDARIES

In some sectors, cooperation may persist, particularly on global challenges like climate change or public health, but always within carefully defined boundaries. In others, particularly around AI, data security, quantum technologies and digital infrastructure, the UK will continue to harden its defences and reduce its exposure. The bilateral relationship will become more transactional, with diplomacy serving as a guardrail against escalation rather than as a platform for deepened trust.

The long-term future may offer moments of recalibration. China's internal economic challenges, demographic pressures, or leadership transitions could alter its global posture. However, so long as the CCP views technological dominance as essential to regime survival, the UK must remain prepared for a strategic environment defined less by mutual accommodation and more by ongoing rivalry, deterrence, and resilience-building. In conclusion, understanding China's ambitions isn't a choice, it's a necessity and the challenge is long-term, serious and already underway"

Heligan Group is an intelligence-led investment and advisory group specialising in partnering with businesses that contribute to global safety and security.

From cyber intrusions to talent recruitment, the Chinese intelligence machine is relentless