Brunel University London

BRUNEL UNIVERSITY RESEARCH CENTRE
Brunel Centre for Intelligence and Security Studies

14 Apr 2023

Issue

1. **Dr Rob Johnson, ...n, n n " ... s .r ' .. 8 estr ^ oc.r p r.**

c.

innovation over human factors such as the volatility of alliances and strategic alignments. It is essential, therefore, to be clear that forecasting the origins or actors from which threats originate is a very different problem from predicting the vectors or shape those threats will take when implemented. However, the latter will inevitably shape the former to a significant degree.

10.

China represents the more radical shift in the threat environment. This is partly because of scale but mainly because China's pursuit of dominance in key emerging technologies such as artificial intelligence (AI) and quantum computing imply very different potential threat vectors from other states, and at very different levels. The most intuitive of these transformations in kinetic threats at the tactical and operational levels from AI-controlled swarms of uncrewed systems that increase agility and accelerate the user's decision cycle. A far more profound shift is presented by the degree to which international competition shifts to a technological competition and economic competition that will decide which geopolitical players will hold the necessary technological advantages.

11. In this context, developments like the PRC's belt-and-road initiative become strategic positioning enterprises, creating alliances of economic alignment and dependence amongst states that the West has difficulty cultivating. Technology acquisition, whether overt, clandestine, or merely concealed by arcane layers of corporate ownership and investment becomes a collective as well as UK national security issue. While scientific and technological espionage may have been Soviet stock in trade during the Cold War, China represents a step change in this type of threat. The Russian 'special services' have attracted the most public attention in the last two decades as much for their paramilitary activities as for espionage and cyber information operations. China, however, has been resourcing its offensive human intelligence (HUMINT) effort, especially through the Ministry of State Security (MSS), on an unprecedented scale. There is also an extensive 'grey' effort at acquiring Western technical know-how through investment in UK and allied research development programmes. China is also engaged in extensive clandestine and 'grey' efforts to interfere in public institutions and policy-making to favour its industrial-technological interests.

12.

The most striking transformation in intelligence priorities currently is, therefore, a renewed emphasis on , covering countersubversion (influence) and countersabotage as welloli [illegible] national security capabilities depends fundamentally on economic prosperity. Under both the and the UK's Security and Intelligence Agencies have a statutory mandate to operate in support of the UK's 'economic wellbeing'. The relationship between Defence Intelligence and 'economic wellbeing', however, is more one of dependence than guardianship. Defence counterintelligence is particularly close to this problem because of the importance of counterintelligence competence in the industrial and technological supply chains. Consequently, counterintelligence needs to be seen as integral to intelligence as a Defence 'Function' as intelligence production to support decision-making and understanding.

Question 2: How have the threats changed, and how could they change further?

14.

18.

Space is now more than just a collection vector for us: it is an arena in which we need to develop domain awareness, and a venue into which our counterintelligence enterprise must expand.

19.

. The barriers to entry into very rich open-source intelligence are extremely low. Any actor with modest resources can buy satellite data, or data derived from satellites at competitive prices. Previously this would have been restricted solely to major states. These capabilities stretch close to ubiquitous technical surveillance. It is deeply worrying that such a wide range of state actors or non-state actors could exploit large data sets for intelligence purposes, developing Insights into our organisations and identifying access points. It is a deeply worrying trend, which we think we will see grow more in the next five years paired with increasing availability from cloud or processing capabilities to extract value from those big data sets.

20.

Everyone carries a very sophisticated sensor for sound, images and locations in their pockets all the time with their mobile phones. With billions of these devices, and their data pull captured by state and commercial

geopolitical events, logistical disruptions or supply chain interdictions. The panel observes that China could potentially leverage its Export Control Law of October 2020 to weaponize logistics. Given Beijing's close ties with Russia, weaponization of the supply chain could negatively impact the UK and other states that support Ukraine.

23. China has capitalized on filling the void of funding, making sweetheart offers to academics or departments. For

cross-government opportunities to work together using the fusion doctrine. From strategic to tactical levels, the China challenge can bring together the MOD, FCDO, and other core groups, alongside academia and commercial entities. It is an opportunity to look at how intelligence of the future should be. A defensive front that includes the UK private tech sector will be beneficial, as many of the problems posed by China can be addressed when the industry works in collaboration with the UK

collection, analysis, and public diplomacy. Investment in and partnership with these sectors should continue to be a priority.

36. Security risks in the private sector posed by hostile foreign powers (HFPs) must be solved collaboratively. The panel anticipates ongoing integration of cloud computing, AI, and web 3.0 (blockchain) into the MOD's intelligence storage, retrieval, analysis, and validation systems. Ukraine, in the middle of an existential emergency, has moved exclusively to cloud because of the security and resilience it offers (it is also cheaper). The panel viewed this shift as inevitable, and the sooner the UK adapts, the better. There are also counterintelligence opportunities to be found in firms which do not qualify for list-x/FSC. These can be targets for threats but also vectors to root them out.

37. With reference to the discussion on countering the belt and road project, intelligence partnerships within the global south must be developed and nurtured to monitor, contain, or even counteract the PRC's expanding influence. The nurturing of new and important relationships will require investment in both attention and personnel. This requires some devotion to specialism within the FCDO and MOD. This effort could be augmented further through partnership with private entities such as defence and security consultancies.

38. . It is at least partly responsible for the UK's outsized influence in diplomatic, security, and geopolitical affairs. We would expect this to continue, however, the UK must plan contingencies for a range of adverse outcomes, especially if American policy returns toward NATO-scepticism, isolationism, or even rapprochement with powers hostile to UK interests. These plans must prepare the MOD for substantial changes in process with respect to foreign liaison. This increased burden also presents opportunities for the UK to lead intelligence partnership among democracies.

39. Where family ties to HFPs or states with whom we are developing closer intelligence ties are often viewed as negative, we may be excluding talent and personnel with access and knowledge to areas of interest. The MOD needs to build vetting practices that allow it to bring 1st generation migrants more easily into service, to harness their languages and cultural knowledge.

40. This is an opportunity to reform vetting and list-x (FSC), so to create and exploit these opportunities. Also, a more technical (and, likely, technologically-driven) approach to information control would enable confidence within the MOD when employing and cooperating with subjects traditionally regarded as "risky."

41. . These decisions must be guided by a clear picture of political (or other material) outcomes. Estonia was cited as an example of a state whose IC prioritises cooperation based on capability. This presents some cultural difficulties though, as it requires both the UK and its partners to concede their own limitations. Beyond that, naturally, the UK's priorities for intelligence partnership should be driven by the national interest and UK policy and strategy.

52.