



# THE HAND OF POLITICS ON BUSINESS

A political risk analysis of the UK National Security and Investment Act 2021

January 2022

**DRD** PARTNERSHIP

# DRD PARTNERSHIP

## Contents

**Introduction ..... 1**

**Methodology ..... 2**

**Advanced Materials ..... 3**

**Advanced Robotics ..... 4**

**Artificial Intelligence..... 5**

**Civil Nuclear ..... 6**

**Communications ..... 7**

**Computing Hardware..... 8**

**Critical Suppliers to Government ..... 9**

**Cryptographic Authentication ..... 10**

**Data Infrastructure..... 11**

**Defence ..... 12**

**Energy ..... 13**

**Military and dual-use technologies ..... 14**

**Quantum Technologies ..... 16**

**Satellite and Space Technology ..... 17**

**Suppliers to the Emergency Services ..... 18**

**Synthetic Biology..... 19**

**Transport..... 20**

## Introduction

The National Security and Investment Act 2021 ('the Act') entered into force on 4 January 2022. It makes investing in 17 designated sectors in the UK subject to direct political control. The Business Secretary has the additional power to review *any* qualifying transaction in any sector if they are concerned an investment may raise national security concerns. While the Government maintains that the UK remains open for business, it is clear that doing deals with a significant UK-angle is no longer going to be the same going forward. And the Act does not only cover foreign acquirers. British acquirers will also be subject to it.

The Secretary of State has discretion to block transactions or to subject them to remedies if they may harm the UK's "national security". There is no appeal on the merits, so getting it right from the first time is key. But what is "national security"? And how will the Secretary of State exercise their discretion?

Some deals are clearly going to pose risks for the UK's national security. Think of a Russian state-owned company acquiring a key supplier to the UK military. But most deals will not be so clear-cut. Serious consideration must therefore be given to what matters in Whitehall and Westminster and the deal should be framed as contributing to those overarching Government objectives. This will help convince the Secretary of State that the deal will not negatively affect the UK's national security.

At the same time, third parties may use the Act to disrupt competitor transactions, raising concerns in Whitehall and Parliament in a way that may cause deals to get snarled up in political bureaucracy. Dealmakers who are concerned about antagonists should be ready to engage on the politics of a deal even more than before.

In this memo, we give a high-level overview of some of the political sensitivities that prevail in the 17 sectors of the economy that have been singled out by the Act. All of these sectors are, of course, sensitive from a UK national security perspective. But some are more sensitive than others, such as the defence and energy sectors, which have been in the policy spotlight for years. Our analysis is necessarily high-level, as each transaction will need to be considered on its individual merits, but we do call out several policy points which we think should be relevant to any deal.

If we can help in any way, please do [get in touch](#).

## WHAT CAN DRD DO?

DRD helps you develop a positive deal rationale that is in line with current Whitehall and Westminster priorities. It also provides strategic public affairs and campaign support to help you get your deal cleared.

## Methodology

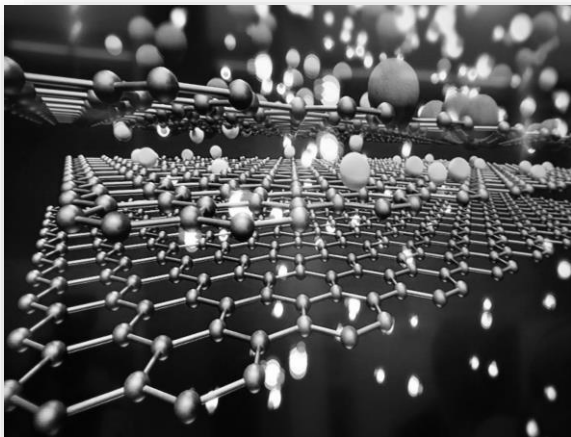
We have assessed the degree of political risk and sensitivity applicable to each of the 17 designated sectors named in the Act. This analysis is drawn from our political intelligence and rooted in policy documents and OSINT research. More specifically, the sensitivity score allocated to each sector is based on an evaluation of the following five criteria:

1. The level of interest to hostile threat actors;
2. The degree and amount of explicit policy statements made by the Government;
3. The applicability of a sector's technology to defence and security interests;
4. The role of a sector in providing critical infrastructure and national resilience; and
5. The parliamentary and political exposure of the sector.



## Advanced Materials

The UK has a long tradition in materials science, and Ministers have sought to make political capital out of notable British breakthroughs, such as Graphene. The production and deployment of Advanced Materials is growing at pace across the UK's defence sector and wider economy. There is a clear risk to national security where a transaction would impair the evolution of Advanced Materials. By increasing functionality, enhancing the ability to maintain products and reducing whole-life costs, Advanced Materials provide significant benefits to military and civilian capabilities. There is a clear risk to national security where a transaction would impair the evolution of Advanced Materials.



By including Advanced Materials as one of the seven technology families of BEIS' Innovation Strategy, the Government identified it as one of the technologies that will help enable the UK to become a science superpower.<sup>1</sup> Part of that designation is a reflection of the wider application of Advanced Materials across the UK's civilian economy, including in the development of 2D materials that can help to deliver more efficient batteries for electric vehicles, and advances in Graphene concrete, which is cheaper and greener to use than regular concrete.<sup>2</sup>

The Government, therefore, recognises this emerging sector's importance to both the defence and civilian industries, as well as to its broader policy goals. Reflecting these sensitivities, the definition of Advanced Materials has undergone careful revision in anticipation of the Act's implementation.

While it is eager to grow the Advanced Materials economy, the Government will also be alive to the risk of these assets being owned by entities with hostile intentions or entities that do not have the same incentives to continue to develop them at pace.

**Political sensitivity rating: 7/10**

<sup>1</sup> [\*BEIS, UK Innovation Strategy—Achieving Vision 2035, Jul 2021.\*](#)

<sup>2</sup> [\*University of Manchester, Roller disco vs climate change: how graphene is transforming the construction industry, Oct 2021.\*](#)



## Advanced Robotics

Domestic research and development of advanced robotics ('AR') products, and a secure international supply of these products, are essential to the UK's national security in both a narrow and a broad sense. In a narrow sense, innovations in AR could unlock important defence and security applications. This is particularly the case for robots that act with some degree of autonomy and can work independently and safely alongside humans. Robots are also used for the inspection, maintenance and repair of nuclear facilities, another sector that is high on the UK's national security radar.

In a broader sense, advances in AR enable the UK to improve its healthcare sector (surgical and nursing robotics), remedy shortages by enhancing logistics, and optimise manufacturing processes. The Covid-19 crisis and ensuing supply shortages, which have not only weakened the UK's economy but also distracted its army, have put a spotlight on how AR can help improve the UK's national security and general resilience in a broader sense.

Notwithstanding that foreign ownership of key AR players could potentially compromise the UK's national security, the Government is very much seeking to grow the sector, including by attracting investment. BEIS has recently emphasised the importance of the UK having a strong AR sector and noted



that this sector has the potential to bring about significant economic changes.<sup>3</sup> Robotics & Smart Machines is also one of the seven technology families featuring in the Government's Innovation Strategy of July 2021, which sought to identify and prioritise technologies that will make the UK a Science and Tech superpower.<sup>4</sup> The multi-sector nature of robotics applications means that the technology draws political interest from a variety of Departments of State, and deals should expect close scrutiny.

Political sensitivity rating: 8/10

<sup>3</sup> [\*BEIS, Economic Impact of Robotics & Autonomous Systems across UK Sectors, Nov 2021—What is RAS?\*](#)

<sup>4</sup> [\*BEIS, UK Innovation Strategy—Achieving Vision 2035, Jul 2021.\*](#)

## Artificial Intelligence

The Artificial Intelligence (AI) industry in the UK is rapidly growing and developing. AI-driven technological progress is predicted to increase UK GDP by 10 per cent in the next decade, which is part of the reason why the Government has a clear ambition to support this sector.<sup>5</sup> In September 2021 the newly established Office for AI unveiled the UK's ten-year national AI strategy, a key purpose of which is to encourage investment in development of AI.<sup>6</sup> In addition, the Government designated AI as one of the technology families in the Innovation Strategy, noting that "remaining among the global leaders will not be easy, with Germany and France making investments that compare to, or exceed, the UK's 2017 AI Sector Deal, and the US and China making enormous investments".<sup>7</sup>



One of the other reasons why the UK wants to develop its homegrown AI-capabilities is that it plays an increasing role in the UK's defence strategy. As noted by the Chief of MI6 in a recent speech: "[the UK's] adversaries are pouring money and ambition into mastering artificial intelligence [...] because they know that mastering these technologies will give them leverage".<sup>8</sup> The nation-state adversaries identified in that speech were China, Russia and Iran.

The National Cyber Security Centre also increasingly relies on AI to detect and counter malicious activity. Human capabilities indeed need to be enhanced by AI to detect, fend off and mitigate the continuous threats from state, criminal and other malicious cyber actors.<sup>9</sup>

With Cyber and Space added to the three existing military domains of Air, Land and Sea, AI has acquired 'frontier status' among political strategists as something the UK should move quickly on to acquire sovereign capability. While the Government is clearly eager to attract investment in the AI sector, it also recognises the risks associated with allowing these technologies to be controlled by foreign entities.

**Political sensitivity rating: 8.5/10**

<sup>5</sup> [The AI Council, \*AI Roadmap—Executive Summary\*, Jan 2021.](#)

<sup>6</sup> [BEIS, \*National AI Strategy\*, Sept 2021.](#)

<sup>7</sup> [BEIS, \*UK Innovation Strategy—Achieving Vision 2035\*, Jul 2021.](#)

<sup>8</sup> [Foreign, Commonwealth & Development Office, \*C's speech to the International Institute for Strategic Studies\*, Nov 2021.](#)

<sup>9</sup> [Cabinet Office, \*National Cyber Strategy 2020\*, Dec 2021.](#)

## Civil Nuclear

Having spent some decades in the wilderness, civil nuclear is back on the agenda and the lax oversight of the Cameron years is now the subject of accelerating policy reversals. As the UK transitions its energy mix to meet net zero targets by 2050, and with power demand expected to grow by at least one third by 2035, nuclear energy generating capacity will only grow in significance. The Government set out its intention to rely on nuclear power in its 2020 long-term nuclear energy strategy<sup>10</sup>, and this was reinforced in the Net Zero Strategy published in October 2021.<sup>11</sup> In addition, the energy crisis of Autumn 2021 highlighted the fragility of the UK's energy supply. It is widely accepted that scaling up nuclear energy is essential to boost domestic energy security.<sup>12</sup>

Ownership of and control over nuclear plants could place entities in a position of significant influence over the UK's economy and resilience. The Government has already been trying to unwind from participation in nuclear projects with the state-owned developer China General Nuclear Power Corp (CGN), which holds a stake in Hinkley Point C, as well as in the planned Sizewell C and Bradwell B plants. This sentiment has been strongly endorsed by the US, which has cited evidence that CGN converts civilian technology to military uses.<sup>13</sup> The removal of CGN from Sizewell or Bradwell, however, means that China could withdraw financing and engineering expertise from Hinkley Point, and that the UK Government could be left without a single nuclear plant by 2030. The Government is currently trying to address this issue by co-funding the development of Rolls-Royce's small modular reactors (SMRs).<sup>14</sup> Investment in SMRs featured in the Government's 2020 Ten Point plan for a Green Industrial Revolution.<sup>15</sup>

The nuclear sector is subject to a much greater level of oversight than many other sensitive industries. As a member state of the International Atomic Energy Agency, and a signatory to the Convention on the Physical Protection of Nuclear Material, the UK is responsible for establishing, implementing and maintaining a high level of physical protection of all civil nuclear facilities. In the nuclear industry, safety is inherently linked to security, as the failure to protect nuclear facilities could have catastrophic consequences.<sup>16</sup>



**Political sensitivity rating: 10/10**

<sup>10</sup> [HM Government, Long-term Nuclear Energy Strategy, March 2013.](#)

<sup>11</sup> [BEIS, Net Zero Strategy: Build Back Greener, Oct 2021.](#)

<sup>12</sup> [Centre for Policy Studies, Bridging the Gap—Executive Summary, June 2020.](#)

<sup>13</sup> Sheppard, David, 'US warns Britain against Chinese alliances on nuclear plants', *Financial Times*, 24 October 2018.

<sup>14</sup> Pfeifer, Sylvia, 'Rolls-Royce mini-nuclear power plant design gets UK state backing', *Financial Times*, 8 November 2021.

<sup>15</sup> [HM Government, The Ten Point Plan for a Green Industrial Revolution, Nov 2020.](#)

<sup>16</sup> [Office for Nuclear Regulation, Security Assessment Principles for the Civil Nuclear Industry, March 2017.](#)



## Communications

The UK's digital economy relies on public electronic communications networks (PECN) and information systems, such as internet and mobile access services, domain name registries, submarine cable systems or public broadcast infrastructure. A change of control over any of these assets is consequently of great interest to the Government.

The security of telecommunications has been of particular interest to the UK Government in recent years, as evidenced by the National Security Council's decision in 2020 to strip out Huawei from the UK's 5G networks. The Telecommunications (Security) Act 2021 implemented the ban on any new Huawei 5G equipment from November 2021 and expanded the duties and powers of the industry's regulator, Ofcom, to oversee providers' compliance with security requirements.<sup>17</sup>

One of the factors behind the Government's clampdown on Huawei in the 5G space was recognition that 5G technologies will increase public reliance on mobile connectivity, facilitating the transition to the Internet of Things and connecting many more devices online. Accordingly, the Parliamentary Defence Committee concluded that 5G increases the risks of "espionage, sabotage or system failure," requiring stricter security requirements for vendors and operators in telecoms.<sup>18</sup> The complexity of hardware and software systems involved in 5G also mean that owners of the network's elements could gain access to other technologies integrated in the infrastructure, such as semiconductor chips.

As the UK's day-to-day systems of housing, transport, energy and finance increasingly rely on PECNs, the failure to protect communication infrastructure could result in society-wide blackouts, bringing down entire sectors of the economy and essential services. As a result, the legislation covers not only service providers and associated facilities, but also submarine cable systems and the providers of repair and maintenance to such systems. Submarine cables account for 95 to 97 per cent of transoceanic digital communications, and the threat of malicious exploitation of their vulnerabilities has been on the Government's radar since the publication of a report by then-backbench MP Rishi Sunak in 2017.<sup>19</sup> Awareness of the risks to the sector remains high within political and military institutional infrastructure.



Political sensitivity rating: 8/10

<sup>17</sup> [UK Public General Acts, Telecommunications \(Security\) Act 2021.](#)

<sup>18</sup> [Defence Committee, \*The Security of 5G\*, Oct 2020.](#)

<sup>19</sup> [Policy Exchange, \*Undersea Cables\*, 2017.](#)

## Computing Hardware

In the area of Computing Hardware, the UK's strengths are in novel, advanced computing hardware manufacturing techniques.<sup>20</sup> The areas of computing hardware that are in scope of the Act include the manufacturing and packaging for use in an electronic circuit of computer processing units and integrated units providing memory. Enterprises that own, create or supply related IP rights are also captured.<sup>21</sup>



The definition of computing hardware is broad and it was suggested during the consultation period that this be narrowed to exclude products that are for consumer use.<sup>22</sup> Whilst some amendments were made to remove unclear terms, the Government also decided that unforeseen 'dual-use' applications of computer hardware could still pose a threat, even in products aimed at consumers.<sup>23</sup> A broad exception has, therefore, not been written into the Act, but the Government has indicated that it does not intend to use the powers to intervene "where the relevant target's products and systems are generally available to the public and for use by consumers".<sup>24</sup> The most obvious way in which harm to national security can occur in this context is if an entity with hostile intentions obtained access to sensitive information and used it to identify or create vulnerabilities in computer hardware products that are used in military applications.

There are, however, also more subtle ways in which harm can occur. Following a change of control in a business, the acquirer may shut down certain lines of research, development or manufacturing that are unprofitable, but also critical to the UK's national security. An acquirer may also prevent key computing hardware products from being made available to companies that use those products to create and build products used for National Security, for example in defence technology.<sup>25</sup>

Political sensitivity rating: 7/10

<sup>20</sup> BEIS, *National Security and Investment: Sectors in Scope of the Mandatory Regime—Computing Hardware*, Jan 2021.

<sup>21</sup> BEIS, *The National Security and Investment Act 2021—Schedule 6 Computing Hardware*, 2021 (further details on which exact computer processing chips and integrated units are in scope are included in the guidance).

<sup>22</sup> BEIS, *National Security and Investment: Sectors in Scope of the Mandatory Regime—Computing Hardware*, Jan 2021.

<sup>23</sup> BEIS, *National Security and Investment: Sectors in Scope of the Mandatory Regime—Computing Hardware*, Jan 2021.

<sup>24</sup> Charles Russell Speechlys, *UK Government extends increased powers for reviewing mergers on national security grounds to additional key strategic sectors*, Aug 2020. (Some proposed changes to the definition were made. These include the removal of the example of silicon as an advanced material, the specific exclusion of "the assembly and packaging of chips and devices into circuit boards" from the definition of "packaging" and the inclusion of a definition of "roots of trust" to mean "hardware, firmware or software components that are inherently trusted to perform critical security functions"). See: BEIS, *The National Security and Investment Act 2021—Schedule 6 Computing Hardware*, 2021.

<sup>25</sup> CMA, *A report to the Secretary of State for DCMS on the acquisition by NVIDIA Corporation of Arm Limited*, July 2020.

## Critical Suppliers to Government

“Critical Suppliers to Government” are those contracted to access very sensitive government data, assets or estates. In practice, the Act will capture firms handling classified information, government security networks and government information systems. Following a public consultation, the definition of “Critical Suppliers” does not include sub-contractors, which some may come to regard as an Achilles’ Heel.<sup>26</sup>

The definition of “Critical Suppliers” clearly captures a vast array of firms. Whether a transaction triggers national security concerns will to a significant degree depend on the precise Government departments the suppliers have contracted with.

Political sensitivity rating: 6/10



---

<sup>26</sup> [BEIS, National Security and Investment Act: Guidance on notifiable acquisitions, Nov 2021.](#)

## Cryptographic Authentication

Cryptographic authentication technology secures sensitive transactions and communications. The Government has identified cryptography as “crucial to the safety and security of UK interests globally”.<sup>27</sup>

BEIS narrowed down its sector definition after consultation, recognising that the initial definition covered a range of companies using the technology simply for consumer devices, software and services. The revised definition makes clear that only entities that research, develop or produce products whose primary function is authentication using cryptographic means, where those products are used in systems that are critical to national security, are in scope.<sup>28</sup>

One potential risk to cryptographic technology that heightens its sensitivity is quantum computing. Quantum computers hold the potential to disrupt cryptographic encryption, meaning that sensitive material under cryptographic encryption may be at risk of exposure to a cryptanalytic attack that is powered by quantum computing technology. The UK Cyber Security Council (UKCSC) indeed highlights the importance of developing quantum-resistant cryptographic technology.<sup>29</sup>



In its Innovation Strategy of July 2021, the Government has demonstrated its desire to enhance investment and innovation in this sector, while calling out the importance of developing secure cryptographic authentication technologies to the UK's national security.<sup>30</sup> Cryptographic authentication has also been identified as vital to protect the UK's cyber security. This area will continue to attract the attention of critical regulators, including the Financial Services Authority, and questions will increasingly be asked regarding control of such technologies.

**Political sensitivity rating: 7/10**

<sup>27</sup> [Cabinet Office, \*National Cyber Strategy 2020\*, Dec 2021.](#)

<sup>28</sup> [BEIS, \*National Security and Investment: Sectors in Scope of the Mandatory Regime—Cryptographic Authentication\*, Jan 2021.](#)

<sup>29</sup> [UK Cyber Security Council, \*NSA and Quantum Cryptography\*, Sept 2021.](#)

<sup>30</sup> [BEIS, \*UK Innovation Strategy—Pillar 4: Missions & Technologies\*, Jul 2021.](#)

## Data Infrastructure

There is evidence that the Government has become increasingly concerned about the security of the country's data infrastructure. The UK is firmly focused on developing a data-centred economy, pledging to "become the world's number one data destination" and "unlock the power of data" as one of its top ten tech priorities.<sup>31</sup> But, at the same time, integration of data into the UK's economic profile requires its infrastructure to be secure – a difficult task in the face of cyber incidents that are only increasing in number, scale and severity.<sup>32</sup>

The sale of data centre operators or cloud storage providers therefore presents the possibility that ill-intentioned third parties could gain access to sensitive information that belongs to Government (central and local), customers and businesses. Such sensitive data could range from bank account details to biometric and medical data, and the loss of control over that data could impact the provision of critical public services. From a policy perspective, shortcomings in national resilience and sovereign capability in this field will only serve to increase the UK's degree of vulnerability to asymmetric attack from hostile actors.

The Government is seeking to ensure the security of this infrastructure because of the important role it plays in the wider economy and delivery of public services. In a policy paper published in November 2021, DCMS emphasised that managed service providers, who supply the data infrastructure that are often the target of attacks, are of paramount importance given the scale of companies moving their operations online.<sup>33</sup> A consultation was launched on that policy paper, calling for views on the framework for introducing security standards for managed service providers.

In addition, DCMS identifies data as a "strategic asset" in its National Data Strategy and lists "ensuring the security and resilience of the infrastructure on which data relies" as a key mission.<sup>34</sup> In its response to a subsequent public consultation, the Government cites the National Security and Investment Act as one of its key tools to manage data infrastructure security.<sup>35</sup>



**Political sensitivity rating: 8/10**

<sup>31</sup> [\*DCMS, Our 10 Tech Priorities, March 2021.\*](#)

<sup>32</sup> [\*National Cyber Security Centre, Annual Review 2021, 2021.\*](#)

<sup>33</sup> [\*DCMS, Call for views on cyber security in supply chains and managed service providers, Nov 2021.\*](#)

<sup>34</sup> [\*DCMS, National Data Strategy, Dec 2020.\*](#)

<sup>35</sup> [\*DCMS, Government response to the consultation on the National Data Strategy, May 2021.\*](#)



## Defence

The UK is NATO's second highest spender on defence. A robust defence sector has unsurprisingly been identified as "vital" to the UK's national security<sup>36</sup>. Investment in companies that have a direct contractual or sub-contractual relationship to the defence of the United Kingdom will therefore face particular scrutiny. The Act's 'Defence' definition highlights the extensive contractual chains that sit behind the supply of the UK's defence sector.<sup>37</sup>

Investments in this sector will be screened for how they affect the UK's security of supply. This is viewed holistically: it is not just about access, but it's about access on competitive terms. Costs of developing new technologies, long-term viability of products, and indeed the viability of the sector as a whole will come into play.<sup>38</sup>

The Government has had a long-standing policy of trying to stay ahead of its principal adversaries when it comes to defence technology.<sup>39</sup> It is expected that the Government will use the Act to strategically curb access to defence technologies by the UK's adversaries if the opportunity arises.

That is not to say that any investment in this sector will be viewed unfavourably. To the contrary, in a policy paper of March 2021 the Ministry of Defence noted that it welcomes overseas investment in the sector and recognised that this will help build capacity, introduce new technology and generate employment for the UK. More generally, the Government seeks to establish a more productive and strategic relationship with the defence industry, with a view to maximising the economic potential of one of the most successful and innovative sectors of British Industry.<sup>40</sup>

The Government is also taking proactive actions to create a more secure defence supply chain. The Defence and Security Accelerator (DASA)<sup>41</sup> finds and funds exploitable innovation to support UK defence and security by brokering meetings between SMEs and private financiers. Its aim is to bring more SMEs into the supply chain. So far 843 innovative proposals worth £136.5mn from 379 organisations have been funded. By helping to fund project development, DASA will gain access to technologies that address predefined challenges in national security, with an aim to stay ahead of the UK's adversaries.<sup>42</sup>

**Political sensitivity rating: 10/10**

---

<sup>36</sup> [\*BEIS, National Security and Investment: Sectors in Scope of the Mandatory Regime—Defence, Jan 2021.\*](#)

<sup>37</sup> [\*Schedule 10 of the Regulations and s. 2\(4\) of the Official Secrets Act 1989.\*](#)

<sup>38</sup> [\*MoD, The Defence and Security Public Contracts Regulations 2011, July 2011.\*](#)

<sup>39</sup> [\*See, most recently, the MoD's 'Defence in a competitive age' policy paper, in which it highlighted the complex and systemic challenges that are posed by Russia, China and Iran and put an emphasis on needing to develop better and faster than these countries: MoD, Global Britain in a competitive age – Strengthening security and defence at home and overseas, March 2021.\*](#)

<sup>40</sup> [\*MoD, Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors—Executive Summary, March 2021.\*](#)

<sup>41</sup> [\*MoD, Innovation for a Safer Future DASA Strategy 2021-2024, May 2021.\*](#)

<sup>42</sup> [\*MoD, Innovation for a Safer Future DASA Strategy 2021-2024—Turning our objectives into reality, May 2021.\*](#)

## Energy

The 2021 energy crisis has heightened political awareness of the increasing role that geopolitics will play in national energy security. Deals involving upstream petroleum and downstream oil facilities, electricity and gas licence holders, electricity generating assets and assets relevant to the supply of fuel in the UK will attract the Government's interest.<sup>43</sup>

Security of supply will be a key area of focus when investment in this sector is screened. The fuel shortages, gas price spikes and bankruptcies of several retail energy suppliers in Q4 2021 brought the UK's energy supply vulnerabilities into sharp focus. Moreover, nearly three-quarters of the UK's energy comes from oil and gas, of which roughly 70 per cent was met by UK Continental Shelf production in 2020.<sup>44</sup> According to research by the former Department of Energy and Climate Change (now BEIS), the infrastructure of regional fuel supply relies on a small number of major sites.<sup>45</sup> Disruption at any of these sites would cause fuel shortages within days. Several events in the last two decades, including the 2005 Buncefield oil storage fire and the 2012 Coryton refinery insolvency, have demonstrated the UK's vulnerability. Ministers will increasingly expect to see evidence of geopolitical de-risking of energy sector deals which go to the heart of the UK's security of supply.

Another factor that will come into play is how investments in this sector will contribute to the UK's strategy of achieving a "net zero" economy by 2050. Electrification is at the core of the UK Net Zero Strategy, and the Government has committed to decarbonising the electricity system by 2035, with the help of low-carbon hydrogen and offshore wind.<sup>46</sup> Deals which offer ways to advance this transition are more likely to be viewed favourably.

General security concerns will also play a role in this sector. The recent acquisition spree of Chinese state-owned companies in renewable energy projects in the UK and the rest of Europe have raised concerns that China can use these assets to exert political influence through its ability to "switch off the lights."<sup>47</sup> Moreover, since Chinese companies are obliged to support Beijing's intelligence-gathering efforts under a 2017 Chinese national security law, analysts are concerned about the ability of Chinese state-owned companies to collect information on customers of their newly acquired subsidiaries.<sup>48</sup>

The energy sector employs around 738,000 people, who work in every part of the UK, meaning that the sector not only has implications for the government's Net Zero strategy, but also for its flagship Levelling Up agenda.<sup>49</sup> A prudent investor in the energy sector will seek to emphasise its track record of positive labour relations and provide reassurances about existing jobs.

**Political sensitivity rating: 10/10**

---

<sup>43</sup> BEIS, *National Security and Investment Act: Guidance on notifiable acquisitions*, Nov 2021.

<sup>44</sup> OGUUK, *Economic Report 2021—Foreword*, 2021.

<sup>45</sup> BEIS, *Government response to consultation of fuel resilience measures*, April 2018.

<sup>46</sup> BEIS, *Net Zero Strategy: Build Back Greener*, Oct 2021.

<sup>47</sup> Oliver, Matt, 'China tightens its grip on UK energy supply: Beijing-controlled firms invest in string of wind farms and nuclear projects', *Daily Mail*, 16 November 2020.

<sup>48</sup> Duxbury, Charles, 'Chinese wind farm investments stoke concerns in Sweden', *Politico*, 26 November 2021.

<sup>49</sup> Energy UK, *Energy sector offers helping hand*, 29 July 2021.

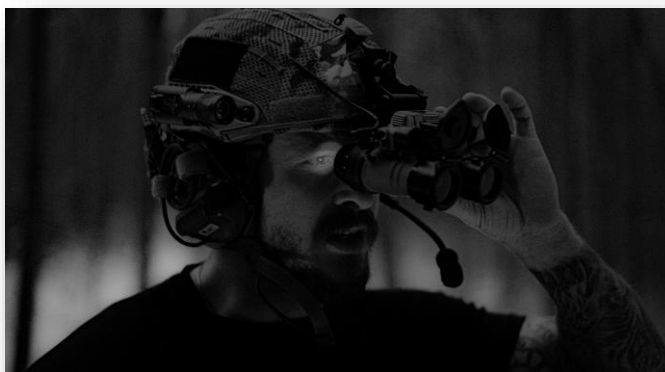
## Military and dual-use technologies

Dual-use technologies are those technologies that have both civilian and military applications, such as GPS; chemical, biological, radiological and nuclear technologies; night vision technology; thermal imaging; drone technology; oscilloscopes; and aluminium pipes.

The Government is looking to protect military and dual-use technologies that are crucial to UK military capabilities or have military applications, such as robotics, artificial intelligence, unmanned and fully automated systems, and quantum computing.<sup>50</sup>

Investments from countries which are viewed as the UK's military and geo-political adversaries, such as China or Russia, will face particular scrutiny. Central government in these countries plays a vital role in driving forward production, as well as research and development, of dual-use technologies for military purposes.<sup>51</sup> To maintain both a military and technological edge, whilst keeping trade secrets and innovation onshore in the UK, the Act will screen any transaction or acquisition which could give the UK's adversaries access to sensitive technology or move the technology abroad.

Particular security concerns exist in relation to China's rapid development efforts to produce world class military and dual-use technologies, as part of a government plan referred to as 'China's Innovation Toolbox'. This innovation toolbox is an effort to leverage new and innovative emerging technology to leapfrog NATO allies in developing the capabilities of the People's Liberation Army.<sup>52</sup>



Under the Enterprise Act 2002, the Business Secretary recently blocked the acquisition of Impcross Limited, a UK-based manufacturer of components for the civilian aerospace industry which also supplies military aircraft manufacturers, by Gardner Aerospace Holdings. Gardner Aerospace Holdings is owned by Shenzhen-listed Ligeance Aerospace Technology Co.<sup>53</sup> The Government specifically identified concerns related to the protection of the UK's aerospace capability, safeguarding of sensitive information, skills and manufacturing capability. Similar concerns would clearly be raised under the new Act.

Finally, the Act interacts closely with the UK's export control legislation and incorporates that regulatory framework into the definition of military and dual-use technologies. Therefore, those sectors of the economy that are familiar with the UK's export control regime, such as leading research universities or those in the defence and manufacturing sectors, will need to be aware of the additional constraints arising from the Act, for example, when such a business or organisation is seeking to raise capital.

---

<sup>50</sup> BEIS, *National Security and Investment: Sectors in Scope of the Mandatory Regime*, March 2021.

<sup>51</sup> *International Institute for Strategic Studies, China's pursuit of advanced dual-use technologies*, Dec 2018.

<sup>52</sup> Arturo G. Munoz, 'Review: Chinese Industrial Espionage. Technology Acquisition and Military Modernization', *Studies in Intelligence*, Vol. 59, No. 4, Dec 2015.

<sup>53</sup> BEIS, *Proposed acquisition of Impcross Ltd by Gardner Aerospace: Undertakings Accepted*, Sept 2020.

Particular concerns are also expected to arise where dual-use technologies are due to be exported to restricted geographies where there is conflict, a threat of terrorism, or a track record of nuclear proliferation, where the Act overlaps with export control rules.<sup>54</sup>



Political sensitivity rating: 9/10

---

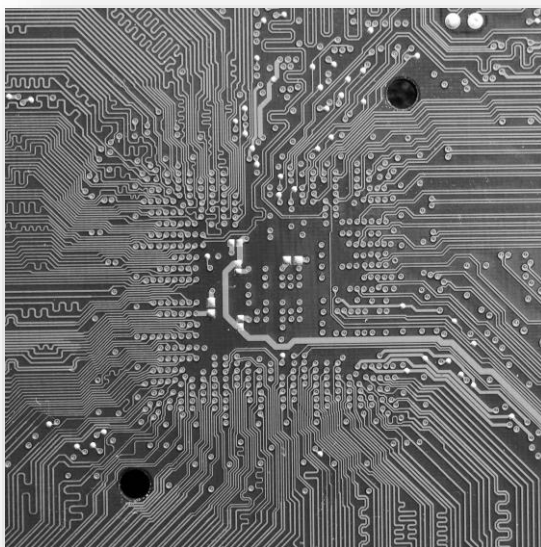
<sup>54</sup> Department for International Trade, [\*UK Strategic Export Control Lists—Introduction\*](#), Jan 2021.

## Quantum Technologies

Because of these wide, varying and developing applications, there is a clear security risk if the UK or its allies do not retain control of this emerging technology. Accordingly, quantum technologies form a key part of the October 2021 AUKUS agreement, which specifically cites them as a key target for the development of “joint capabilities” between the UK, the US and Australia<sup>55</sup>. BEIS also very recently announced a separate statement of intent for collaboration between the UK and US on quantum science and technologies<sup>56</sup>.

Domestic policy is focused on supporting and protecting the development of quantum technologies. The Chief of MI6 noted in a recent speech how “our adversaries are pouring money and ambition into mastering...quantum computing, because they know that mastering these technologies will give them leverage.”<sup>57</sup> The Government’s Innovation Strategy includes quantum computing as one of the seven families of UK strength and opportunity, which means that there will be an enhanced focus on collaboration between industry, researchers and the Government in order to develop a strong domestic industry in this space.<sup>58</sup>

Political sensitivity rating: 9/10



---

<sup>55</sup> [House of Commons Library, \*The AUKUS agreement\*, Oct 2021.](#)

<sup>56</sup> [BEIS, \*New joint statement between UK and US to strengthen quantum collaboration\*, Nov 2021.](#)

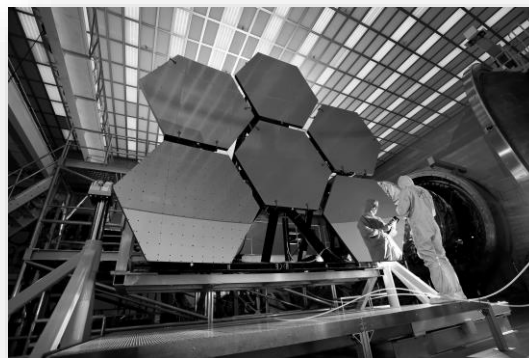
<sup>57</sup> [Foreign, Commonwealth & Development Office, \*C's speech to the International Institute for Strategic Studies\*, Nov 2021.](#)

<sup>58</sup> [BEIS, \*UK Innovation Strategy—Pillar 4: Missions & Technologies\*, Jul 2021.](#)



## Satellite and Space Technology

The UK space industry generates a domestic income of £14.86bn annually according to the Integrated Review.<sup>59</sup> The Ministry of Defence established a new Space Command Headquarters in August 2021 and the related Integrated Review reaffirms the UK's desire to capture 10 per cent of the global space market.<sup>60</sup>



The Government is taking an interest in regulating this sector with four main pillars in mind, namely growing the UK's share of the space economy, collaborating internationally with partners, growing the UK's role as a science and technology superpower, and developing resilient space capabilities and services.<sup>61</sup>

The fourth pillar is key for present purposes. Specifically, secure global communications facilitated by satellites ensure connectivity to remote and rural communities across the country. Satellite-derived position, navigation and timing signals underpin services such as banking, transportation and most of the UK's critical national infrastructure for the energy, policing and healthcare sectors. Satellite communication links and space-derived data for defence purposes support the use of signals intelligence, i.e. military intelligence concerned with the monitoring, interception and interpretation of radio and radar signals.<sup>62</sup> Any prospective buyer of satellite and space technology assets will need to bear this context in mind when developing its deal rationale and advocacy.

In 2019, the UK Government issued a public interest intervention notice under the Enterprise Act 2002 to review a \$6bn takeover of British satellite company Inmarsat on national security grounds due to concerns that sensitive technology and other assets could be snapped up by a consortium of US, Canadian and UK buyers. The intervention was made to keep engineering jobs, a key facility and R&D for Inmarsat, located in the UK, and the buyers were indeed forced to give commitments to that effect to get their deal cleared.<sup>63</sup> Ministers can be expected to adopt an analogous approach under the new Act.

Political sensitivity rating: 8/10

<sup>59</sup> [UK Space Agency, Space Growth Action Plan, April 2014.](#)

<sup>60</sup> [BEIS, National Space Strategy, Sept 2021.](#)

<sup>61</sup> [BEIS, National Space Strategy, Sept 2021.](#)

<sup>62</sup> [BEIS, National Space Strategy, Sept 2021.](#)

<sup>63</sup> [DCMS, Inmarsat Public Interest Intervention Notice, July 2019.](#)

## Suppliers to the Emergency Services

The Emergency Services sector is comprised of the agencies that help to preserve the UK's national security during times of distress. These include the Fire and Rescue, Ambulance and Police Services, the MoD, and the Border Force, but also services of equal importance that may have a slightly more under-the-radar profile, such as the Civil Nuclear Constabulary.<sup>64</sup>

The Government has previously recognised the security implications if this sector fell into the control of adverse international hands: the Emergency Services are one of the thirteen sectors that comprise the country's Critical National Infrastructure.<sup>65</sup> In addition, the Cabinet Office's Public Summary of Sector Security and Resilience Plans lays out that loss of communications and loss of power are the most prominent risks that face the sector.<sup>66</sup>

The centrality of communications services was recently also reflected in the Competition and Market Authority's decision to open a market investigation into Motorola's Airwave network.<sup>67</sup> Taken together, the Government and independent regulators are therefore of the view that the status of suppliers to the Emergency Services presents political sensitivities given that they could threaten the ability of the state to provide essential services at a critical time.

Political sensitivity rating: 7/10



<sup>64</sup> [BEIS, \*National Security and Investment Act: Guidance on notifiable acquisitions—Suppliers to the Emergency Services\*, Nov 2021.](#)

<sup>65</sup> [National Cyber Security Centre, \*CNI Hub\*, 2021.](#)

<sup>66</sup> [Cabinet Office, \*Public Summary of Sector Security and Resilience Plans\*, Dec 2017.](#)

<sup>67</sup> [Competition and Markets Authority, \*CMA Opens investigation into Motorola's Airwave network\*, Oct 2021.](#)

## Synthetic Biology

Synthetic biology is the design or creation of biological components such as enzymes, genetic circuits, cells and systems that do not exist naturally. This includes gene editing, cloning and using DNA for storing data or bio-enabled computing.<sup>68</sup>

Synthetic Biology was previously defined as “Engineering Biology” in earlier versions of the draft Act, but had its scope narrowed following consultation responses from industry arguing that ‘Engineering Biology’ was too broad.<sup>69</sup> The definition of “Synthetic Biology” is now much more precise and contains a number of exceptions.<sup>70</sup>

Bio-engineering techniques can be used in several ways that are adverse to the UK’s national security. Advancements in biological manipulation have the potential to be used to develop bioweapons that are used in bioterrorism to recreate pathogenic viruses, engineer bacteria to make them more dangerous or engineer microbes to produce and release toxins and biochemicals.<sup>71</sup> Bio-computing, which seeks to use cells to enhance computing functions due to their superior computing capabilities, could be used to hack into Government IT systems.

Clear national security risks would emerge if ill-intentioned entities take control of research and manufacturing in the UK, or gain access to insights that could be used against the UK.<sup>72</sup> More indirectly, anti-competitive acquisitions could stifle advancements in this area, leaving the UK behind in its development and understanding of the sector, and as a result harming its ability to defend against biological threats.



This is an emerging area from a policy perspective, and the shifting sands during the consultation exercise reflect a degree of ‘exploratory thinking’ by Ministers and officials which may only coalesce as the Act plays out in practice.

**Political sensitivity rating: 7/10**

---

<sup>68</sup> [\*The National Security and Investment Act 2021 \(Notifiable Acquisition\) \(Specification of Qualifying Entities\) Regulations 2021—Synthetic Biology, 2021.\*](#)

<sup>69</sup> [\*The National Security and Investment Act 2021 \(Notifiable Acquisition\) \(Specification of Qualifying Entities\) Regulations 2021—Synthetic Biology, 2021.\*](#)

<sup>70</sup> The definition is however still regarded as being very broadly defined and there are concerns that this could negatively impact businesses in the life sciences sector. This risks imposing long processes for biotech organisations seeking funding, which will have knock-on implications for developing and manufacturing lifesaving medicines. A paragraph of exceptions relating to ‘human or veterinary medicines or immunomodulatory approaches’ was added in an attempt to mitigate this risk. See: [\*BIA, Government defines Synthetic Biology for National Security and Investment regime, July 2021\*](#) and [\*BEIS, National Security and Investment: Sectors in Scope of the Mandatory Regime – Synthetic Biology, March 2021.\*](#)

<sup>71</sup> Cross, Ryan, ‘[Synthetic biology could enable bioweapons development](#)’, *C&EN*, 19 June 2018.

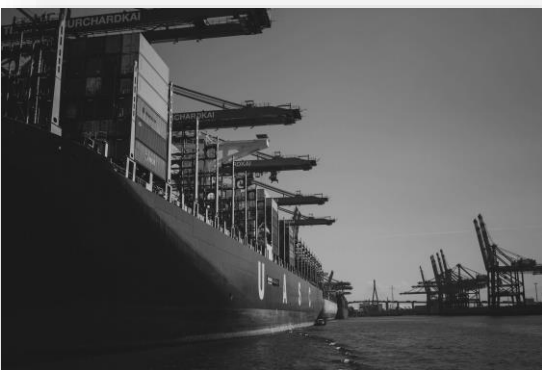
<sup>72</sup> [\*BEIS, National Security and Investment: Sectors in Scope of the Mandatory Regime – Engineering Biology, March 2021.\*](#)

## Transport

Transport has been identified as a key sector contributing to economic prosperity and security across the United Kingdom and has, as a result, been included in the Act. However, not all activities in the transport sector are deemed to be sufficiently sensitive to be subject to mandatory notification. The Act focuses on key infrastructure in the maritime, aviation and air traffic control sectors, such as ports and harbours, or airports as defined in the Civil Aviation Act.<sup>73</sup> Additionally, only investment in infrastructure which is sufficiently large will be caught by the Act. For instance, ports and harbours which handle 1 million tonnes of cargo, or airports handling at least six million passengers or 100,000 tonnes of freight are in scope.<sup>74</sup>

As in other sectors of the economy, there is a balance to be struck between national security and maintaining open trading relationships with major economic players such as China, the US, the EU, and the Gulf States. Previous investments by a Chinese sovereign wealth fund, China Investment Corporation (CIC) in Heathrow Airport, Thames Water and Royal Albert Dock, which breezed through at the time, would today be reviewed under the Act. It is expected that deals like these would attract a significant degree of scrutiny, following the Government's desire to curb Chinese influence over British business by establishing the British International Investment arm, a development fund designed to provide transparent investments as an alternative to China.<sup>75</sup> The purchase of six major seaports in the USA by Emirati enterprise, Dubai Ports World ("DP World") in 2006 was met with concern in the US due to fears that the federal government failed to consider vulnerabilities which these purchases may create, such as terrorism or loss of control of US assets to a state-owned enterprise.<sup>76</sup>

The National Infrastructure Strategy details plans to invest in transport infrastructure as part of a wider strategy to level up the country, including allocating £200mn to invest in a Port Infrastructure Fund to ensure that the UK is equipped with the infrastructure necessary to fulfil its international trade objectives as part of its Global Britain strategy.<sup>77</sup>



Additionally, investment in freeports as part of the Government Freeport Strategy aims to establish national hubs for global trade and investment across the UK. Freeports will receive a combination of tariff benefits, tax incentives, and regeneration funding.<sup>78</sup> These strategies come at a significant financial cost to the Government. The UK will have to consider whether it undergoes a decoupling from Chinese investment in the transport sector, due to national

---

<sup>73</sup> Section 66(1) of the [Civil Aviation Act 2012](#).

<sup>74</sup> [BEIS, National Security and Investment: Sectors in Scope of the Mandatory Regime, March 2021](#).

<sup>75</sup> Hughes, Laura, 'UK seeks to counter China's influence with new development arm', *Financial Times*, 24 November 2021

<sup>76</sup> E.Flynn, Stephen, 'The DP World Controversy and the Ongoing Vulnerability of US Seaports Council on Foreign Relations', *Council on Foreign Relations*, 2 March 2006.

<sup>77</sup> [HM Treasury, National Infrastructure Strategy, Nov 2020](#).


<sup>78</sup> [House of Commons Library, Government policy on freeports, Nov 2021](#).

security and political factors, or whether it is better to opt for greater investment from China to save government expenditure.

As a further example of this tension, the Aviation Strategy, published by the Government, talks up the benefits of some foreign investment from countries such as China, referencing job creation and a boost in export values of £1.29 bn passing through Manchester Airport.<sup>79</sup> The strategy details the vital role of Chinese investment, noting an eastward shift in global aviation markets.<sup>80</sup> China will continue to grow as a dominant player in the aviation industry and it seems that the UK will remain open to investments which create sustainable growth in the sector.

Still in the aviation sector, Transport Secretary has recently made a clear commitment at the Dubai World Expo to work with the UAE to drive innovation, decarbonise transport and create green jobs at the Dubai World Expo.<sup>81</sup> Such policy commitments will come into play under the new Act when UAE entities seek to invest in the UK aviation market.

Transport also plays a key part in the Government's Net Zero Strategy.<sup>82</sup> Where an investment in infrastructure supports carbon neutral aircraft technology, or sustainable aviation fuels at airports, or the use of zero emission HGVs to move freight from ports, it is likely to receive an easier ride under the Act.



Political sensitivity rating: 7.5/10

---

<sup>79</sup> *HM Government, Aviation 2050: The future of UK aviation, Dec 2018.*

<sup>80</sup> *HM Government, Aviation 2050: The future of UK aviation, Dec 2018.*

<sup>81</sup> *Department for Transport, Transport Secretary to set out commitments to UK investment and job creation at World Expo in Dubai, Nov 2021.*

<sup>82</sup> *BEIS, Net Zero Strategy: Build Back Greener, Oct 2021.*





## DRD PARTNERSHIP

### BUILDING AND PROTECTING REPUTATIONS

DRD is a strategic communications consultancy focused on building value for our clients and protecting their reputations at moments of challenge and change.

**T:** + 44 (0 )203 951 0346

**T:** +44 (0) 7775 530 978 (Jon McLeod, Partner)

**W:** [www.drdpartnership.com](http://www.drdpartnership.com)

**A:** DRD Partnership, 17 Slingsby Place, St Martin's Courtyard, London WC2E 9AB